日本国特許庁

13.09.00

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１２月　２日

出願番号
Application Number: 平成１１年特許願第３４３７０７号

出願人
Applicant (s): 富士通株式会社
日本コロムビア株式会社
三洋電機株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年１０月２０日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８５４４１

【書類名】　特許願

【整理番号】　1991489

【提出日】　平成11年12月 2日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 11/08

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畑中　正行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　蒲田　順

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畠山　卓久

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　古田　茂樹

【発明者】
【住所又は居所】　東京都港区赤坂四丁目１４番１４号　日本コロムビア株式会社内
【氏名】　穴澤　健明
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　日置　敏昭
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　金森　美和
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　堀　吉宏
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【特許出願人】
【識別番号】　000004167
【住所又は居所】　東京都港区赤坂四丁目１４番１４号
【氏名又は名称】　日本コロムビア株式会社
【特許出願人】
【識別番号】　000001889
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号
【氏名又は名称】　三洋電機株式会社

【代理人】

【識別番号】　100064746

【弁理士】

【氏名又は名称】　深見　久郎

【選任した代理人】

【識別番号】　100085132

【弁理士】

【氏名又は名称】　森田　俊雄

【選任した代理人】

【識別番号】　100091409

【弁理士】

【氏名又は名称】　伊藤　英彦

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第243583号

【出願日】　平成11年 8月30日

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ再生装置

【特許請求の範囲】

【請求項１】　暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツキーを復号するための第１の復号鍵を保持する第１の鍵保持部と、

前記データ格納部からの前記暗号化コンテンツキーを基にして、前記第１の鍵保持部からの出力により復号処理を行なうことで、前記コンテンツキーを抽出する第１の復号処理部と、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、前記第１の復号処理部の出力により復号してコンテンツデータを抽出するための第２の復号処理部を含む、データ再生装置。

【請求項２】　前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスする毎に更新される第１のセッションキーを生成する第１のセッションキー発生部と、

前記第１のセッションキーを前記データ格納部にて復号可能な第１の暗号鍵で暗号化して前記データ格納部に与えるための第１の暗号化処理部と、

前記第１のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第１のセッションキーについて復号して前記第１の復号処理部に与える第３の復号処理部をさらに含む、請求項１記載のデータ再生装置。

【請求項３】　前記データ再生部は、前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに異なる第２のセッションキーを、さらに、前記第１の復号鍵により復号可能な暗号化を施して供給を受け、

前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに更新される第１のセッションキーを生成する第１のセッションキー発生部と、

前記第１のセッションキーを、外部から入力されたデータから前記第１の複合鍵に基づいて前記第１の復号処理部にて抽出された前記第２のセッションキーで暗号化して前記データ格納部に与えるための第２の暗号処理部と、

前記第１のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第１のセッションキーについて復号して前記第１の復号処理部に与える第３の復号処理部をさらに含む、請求項１記載のデータ再生装置。

【請求項４】　前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項１～３のいずれか１項に記載のデータ再生装置。

【請求項５】　前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記憶部と、

前記第１の暗号化鍵を保持する第２の鍵保持部と、

前記第１の暗号化鍵により暗号化されたデータを復号するための第２の復号鍵を保持するための第３の鍵保持部と、

前記第２の復号鍵に基づいて、前記データ再生部から前記第１の暗号化鍵により暗号化されて伝達された前記第１のセッションキーを復号するための第４の復号処理部と、

前記第４の復号処理部で抽出された前記第１のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第２の暗号化処理部を備える、請求項２記載のデータ再生装置。

【請求項６】　前記データ格納部は、

前記データ格納部に与えられるデータを保持するための記録部と、

前記暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第２のセッションキーを発生する第２のセッションキー発生部と、

前記第１の復号鍵にて復号可能な第２の暗号化鍵により、暗号化処理を行なう第３の暗号化処理部と、

前記第２のセッションキーに基づいて、前記データ再生部から前記第２のセッションキーにて暗号化されて伝達された前記第１のセッションキーを復号するための第５の復号処理手段と、

前記第５の復号処理手段にて抽出された前記第１のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第４の暗号化処理部を備える、請求項３記載のデータ再生装置。

【請求項７】　前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項５または６記載のデータ再生装置。

【請求項８】　前記データ再生部は、

少なくとも前記第１の鍵保持部と、前記第１の復号処理部と、前記第２の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている、請求項１記載のデータ再生装置。

【請求項９】　前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項１～４のいずれか１項に記載のデータ再生装置。

【請求項１０】　暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを保持し、かつ、前記データ再生装置に着脱可能なデータ格納部と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生す

るためのデータ再生部とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、復号してコンテンツデータを抽出するための第１の復号処理部と、

認証データを認証鍵により復号可能な暗号化を施して保持し前記データ格納部に対して出力可能な認証データ保持部とを含み、

前記データ格納部は、

前記認証鍵により暗号化されて前記データ再生部から与えられる前記認証データを復号して抽出するための第２の復号処理部と、

前記第２の復号処理部により抽出された前記認証データに基づいて認証処理を行う制御手段とを含む、データ再生装置。

【請求項１１】　前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツキーの取得のためにアクセスする毎に更新されるセッションキーを生成するセッションキー発生部と、

前記セッションキーを前記データ格納部にて復号可能な第１の暗号鍵で暗号化して前記データ格納部に与えるための暗号化処理部と、

前記第１のセッションキーで暗号化されて前記データ格納部から受信した前記コンテンツキーを、前記第１のセッションキーについて復号する第３の復号処理部をさらに含む、請求項１０記載のデータ再生装置。

【請求項１２】　前記認証データ保持部は、第１の復号鍵で復号可能な暗号化を施す第２の暗号鍵を前記認証データとともに前記認証鍵により復号可能な暗号化を施して保持し、前記データ格納部に対して出力し、

前記第３の復号処理部は、前記第２の暗号鍵で暗号化された上で前記データ格納部から受信した前記第１の暗号化鍵を、前記第１の復号鍵にて復号し、前記暗号化処理部に与える第４の復号処理部を備える、請求項１１記載のデータ再生装置。

【請求項１３】　前記第４の復号処理部は、さらに、

前記第１の復号鍵で復号可能な第２の暗号鍵で暗号化され、さらに前記セッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキー

を、前記第３の復号処理部にて前記セッションキーについて復号し、得られた前記第２の暗号化鍵にて暗号化された前記コンテンツキーを入力として、前記第１の復号鍵にて復号し、前記第１の復号処理部に与える、請求項１１記載のデータ再生装置。

【請求項１４】　前記データ再生部は、

さらに、予め定められた第２復号鍵にて復号する第５の復号処理部を備え、

前記第５の復号処理部は、

前記第４の復号鍵で復号可能な暗号化を施されて、さらに前記セッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキーを、前記第３の復号部にて前記セッションキーについて復号し、得られた第４の復号鍵で復号可能な暗号化を施された前記コンテンツキーを入力とし、

前記第２の復号鍵にて復号し、前記第１の復号処理部に与える、請求項１１または１２記載のデータ再生装置。

【請求項１５】　前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項１０～１４のいずれか１項に記載のデータ再生装置。

【請求項１６】　前記データ再生装置は、さらに、簡易携帯電話網を含む携帯電話網に接続するインタフェースを備える、請求項１０～１４のいずれか１項に記載のデータ再生装置。

【請求項１７】　前記データ再生装置は、さらに、前記インタフェースを介して通話を行なう通話処理部を備える、請求項１６記載のデータ再生装置。

【請求項１８】　前記データ格納部は、前記データ再生部に対して着脱可能である、請求項１７に記載のデータ再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

【０００２】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽データや画像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】

したがって、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

【発明が解決しようとする課題】

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権データの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

【０００７】

このような記録装置としては、たとえば、メモリカードのように電気的にデータの書込および消去が可能な媒体が用いられることになる。

【０００８】

さらに、配信データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

【０００９】

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティ対策を施す必要がある。

【００１０】

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができるとすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来たすことになる。

【００１１】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

【００１２】

【課題を解決するための手段】

請求項１記載のデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部と、データ格納部からの出力を受けて、暗号化コンテンツデータを再生するためのデータ再生部とを備え、データ再生部は、データ格納部から読み出された暗号化コンテンツキーを復号

するための第１の復号鍵を保持する第１の鍵保持部と、データ格納部からの暗号化コンテンツキーを基にして、第１の鍵保持部からの出力により復号処理を行なうことで、コンテンツキーを抽出する第１の復号処理部と、データ格納部から読み出された暗号化コンテンツデータを受けて、第１の復号処理部の出力により復号してコンテンツデータを抽出するための第２の復号処理部を含む。

【００１３】

請求項２記載のデータ再生装置は、請求項１記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスする毎に更新される第１のセッションキーを生成する第１のセッションキー発生部と、第１のセッションキーをデータ格納部にて復号可能な第１の暗号鍵で暗号化してデータ格納部に与えるための第１の暗号化処理部と、第１のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第１のセッションキーについて復号して第１の復号処理部に与える第３の復号処理部をさらに含む。

【００１４】

請求項３記載のデータ再生装置は、請求項１記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに異なる第２のセッションキーを、さらに、第１の復号鍵により復号可能な暗号化を施して供給を受け、データ再生部は、データ格納部に対して暗号化コンテンツデータの取得のためにアクセスするごとに更新される第１のセッションキーを生成する第１のセッションキー発生部と、第１のセッションキーを、外部から入力されたデータから第１の複合鍵に基づいて第１の復号処理部にて抽出された第２のセッションキーで暗号化してデータ格納部に与えるための第２の暗号処理部と、第１のセッションキーでさらに暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、第１のセッションキーについて復号して第１の復号処理部に与える第３の復号処理部をさらに含む。

【００１５】

請求項４記載のデータ再生装置は、請求項１～３のいずれか１項に記載のデータ再生装置の構成に加えて、コンテンツデータは、データ量を削減するための符

号化方式にて符号化された符号化音楽データであって、データ再生部は、符号化音楽データから符号化方式に基づいて音楽データを再生する音楽再生部と、再生した音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む。

【００１６】

請求項５記載のデータ再生装置は、請求項２記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記憶部と、第１の暗号化鍵を保持する第２の鍵保持部と、第１の暗号化鍵により暗号化されたデータを復号するための第２の復号鍵を保持するための第３の鍵保持部と、第２の復号鍵に基づいて、データ再生部から第１の暗号化鍵により暗号化されて伝達された第１のセッションキーを復号するための第４の復号処理部と、第４の復号処理部で抽出された第１のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第２の暗号化処理部を備える。

【００１７】

請求項６記載のデータ再生装置は、請求項３記載のデータ再生装置の構成に加えて、データ格納部は、データ格納部に与えられるデータを保持するための記録部と、暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第２のセッションキーを発生する第２のセッションキー発生部と、第１の復号鍵にて復号可能な第２の暗号化鍵により、暗号化処理を行なう第３の暗号化処理部と、第２のセッションキーに基づいて、データ再生部から第２のセッションキーにて暗号化されて伝達された第１のセッションキーを復号するための第５の復号処理手段と、第５の復号処理手段にて抽出された第１のセッションキーにより、記憶部に保持されたデータを暗号化して出力するための第４の暗号化処理部を備える。

【００１８】

請求項７記載のデータ再生装置は、請求項５または６記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能なメモリカードである。

【００１９】

請求項８記載のデータ再生装置は、請求項１記載のデータ再生装置の構成に加えて、データ再生部は、少なくとも第１の鍵保持部と、第１の復号処理部と、第２の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている。

【００２０】

請求項９記載のデータ再生装置は、請求項１～４のいずれか１項に記載のデータ再生装置の構成に加えて、データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる。

【００２１】

請求項１０記載のデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのコンテンツキーを保持し、かつ、データ再生装置に着脱可能なデータ格納部と、データ格納部からの出力を受けて、暗号化コンテンツデータを再生するためのデータ再生部とを備え、データ再生部は、データ格納部から読み出された暗号化コンテンツデータを受けて、復号してコンテンツデータを抽出するための第１の復号処理部と、認証データを認証鍵により復号可能な暗号化を施して保持しデータ格納部に対して出力可能な認証データ保持部とを含み、データ格納部は、認証鍵により暗号化されてデータ再生部から与えられる認証データを復号して抽出するための第２の復号処理部と、第２の復号処理部により抽出された認証データに基づいて認証処理を行う制御手段とを含む。

【００２２】

請求項１１記載のデータ再生装置は、請求項１０記載のデータ再生装置の構成に加えて、データ再生部は、データ格納部に対して暗号化コンテンツキーの取得のためにアクセスする毎に更新されるセッションキーを生成するセッションキー発生部と、セッションキーをデータ格納部にて復号可能な第１の暗号鍵で暗号化してデータ格納部に与えるための暗号化処理部と、第１のセッションキーで暗号化されてデータ格納部から受信したコンテンツキーを、第１のセッションキーについて復号する第３の復号処理部をさらに含む。

【００２３】

請求項１２記載のデータ再生装置は、請求項１１記載のデータ再生装置の構成に加えて、認証データ保持部は、第１の復号鍵で復号可能な暗号化を施す第２の暗号鍵を認証データとともに認証鍵により復号可能な暗号化を施して保持し、データ格納部に対して出力し、第３の復号処理部は、第２の暗号鍵で暗号化された上でデータ格納部から受信した第１の暗号化鍵を、第１の復号鍵にて復号し、暗号化処理部に与える第４の復号処理部を備える。

【００２４】

請求項１３記載のデータ再生装置は、請求項１１記載のデータ再生装置の構成に加えて、第４の復号処理部は、さらに、第１の復号鍵で復号可能な第２の暗号鍵で暗号化され、さらにセッションキーで暗号化された上でデータ格納部から受信したコンテンツキーを、第３の復号処理部にてセッションキーについて復号し、得られた第２の暗号化鍵にて暗号化されたコンテンツキーを入力として、第１の復号鍵にて復号し、第１の復号処理部に与える。

【００２５】

請求項１４記載のデータ再生装置は、請求項１１または１２記載のデータ再生装置の構成に加えて、データ再生部は、さらに、予め定められた第２復号鍵にて復号する第５の復号処理部を備え、第５の復号処理部は、第４の復号鍵で復号可能な暗号化を施されて、さらにセッションキーで暗号化された上でデータ格納部から受信したコンテンツキーを、第３の復号部にてセッションキーについて復号し、得られた第４の復号鍵で復号可能な暗号化を施されたコンテンツキーを入力とし、第２の復号鍵にて復号し、第１の復号処理部に与える。

【００２６】

請求項１５記載のデータ再生装置は、請求項１０～１４のいずれか１項に記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能なメモリカードである。

【００２７】

請求項１６記載のデータ再生装置は、請求項１０～１４のいずれか１項に記載のデータ再生装置の構成に加えて、データ再生装置は、さらに、簡易携帯電話網

を含む携帯電話網に接続するインタフェースを備える。

【００２８】

請求項１７記載のデータ再生装置は、請求項１６記載のデータ再生装置の構成に加えて、データ再生装置は、さらに、インタフェースを介して通話を行なう通話処理部を備える。

【００２９】

請求項１８記載のデータ再生装置は、請求項１７記載のデータ再生装置の構成に加えて、データ格納部は、データ再生部に対して着脱可能である。

【００３０】

【発明の実施の形態】

［実施の形態１］

［システムの全体構成］

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【００３１】

なお、以下では携帯電話網を介して、暗号化された音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、暗号化された他の著作物情報データ、例えば画像データ等の著作物情報データを、復号して平文化して再生することが可能なものである。

【００３２】

なお、ここで携帯電話網としては、ＰＨＳ（Personal Handy Phone）などの簡易携帯電話網も含むものとする。

【００３３】

図１を参照して、著作権の存在する音楽データを管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア２０である携帯電話会社に、このような暗号化データを与える。

【００３４】

配信キャリア２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。配信サーバ１０は、配信リクエストがあると、要求された暗号化音楽情報を携帯電話会社２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【００３５】

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１４０等を介してこのような再生された音楽データを聴取することが可能である。

【００３６】

以下では、このような配信サーバ１０と配信キャリア（携帯電話会社）２０とを併せて、音楽サーバ３０と総称することにする。

【００３７】

また、このような音楽サーバ３０から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【００３８】

しかも、配信キャリア２０において、たとえば１曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００３９】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【００４０】

［配信サーバ１０の構成］

図１において配信サーバ１０は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したコンテンツデータやコンテンツキー等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、暗号化コ

ンテンツデータを復号するためのコンテンツキーＫｃを公開暗号化鍵ＫＰｐにより暗号化するためのコンテンツキー暗号化処理部３１６と、配信情報データベース３０４および課金データベース３０２とデータバスＢＳ１を介してデータ授受を行ない、配信サーバ１０の動作を制御するためのコントローラ３１２と、通信網を介して、配信サーバ１０と配信キャリア２０との間でデータ授受を行なうための通信装置３５０とを備える。

【００４１】

すなわち、配信情報データベース３０４からは、コンテンツデータＤｃが、復号鍵であるコンテンツキーＫｃにより復号可能な状態に暗号化された暗号化コンテンツデータ［Ｄｃ］Ｋｃと、コンテンツキーＫｃとが出力される。コントローラ３１２は、コンテンツキー暗号化処理部３１６を制御して、このコンテンツキーＫｃを公開暗号化鍵ＫＰｐにより暗号化した［Ｋｃ］Ｋｐを通信装置３５０を介して、配信キャリア２０に与える。

【００４２】

ここで、［Ｙ］Ｘという表記は、データＹを、キー（鍵）Ｘにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

【００４３】

［端末（携帯電話機）の構成］

図２は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００４４】

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、外部からの指示を携帯電話機１００に与えるためのタッチキーやダイヤルキーなどを含むキーボード１１０８と、コント

ローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを備える。

【００４５】

携帯電話機１００は、さらに、サーバ３０からの暗号化コンテンツデータ［Ｄｃ］Ｋｃおよび暗号化コンテンツキー［Ｋｃ］Ｋｐを格納するためのメモリ１１０と、音楽再生モジュール１５００とを備える。この音楽再生モジュール１５００は、公開暗号化鍵ＫＰｐに対応し、キーＫＰｐで暗号化されたデータを復号可能な秘密復号鍵Ｋｐを保持するＫｐ保持部１５４０と、音楽サーバ３０から伝送され公開暗号化鍵ＫＰｐにより暗号化コンテンツキー［Ｋｃ］Ｋｐをメモリ１１０から受けて復号するための復号処理部１５３０と、音楽サーバ３０から配信されメモリ１１０中に格納された暗号化コンテンツデータ［Ｄｃ］Ｋｃを、復号処理部１５３０で復号抽出されたコンテンツキーＫｃに基づいて復号するための復号処理部１５２０と、復号処理部１５２０からの復号されたコンテンツデータを受けて、コンテンツデータを符号化した符号化方式、例えば
ＭＰ３、ＡＣ３等のデジタル圧縮符号化方式の再生手順に従って音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２とを含む。

【００４６】

携帯電話機１００は、さらに、デジタルアナログ変換部１５１２の出力を受けて、ヘッドホン１４０と接続するための接続端子１５１４とを含む。

【００４７】

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【００４８】

また、図２に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０および復号処理部１５２０を、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組み込む構成とすることが可能である。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

【００４９】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機１００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【００５０】

さらに、図２において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

【００５１】

［再生処理］

図３は、携帯電話機１００内において、メモリ１１０に保持された暗号化コンテンツデータから、コンテンツデータを復号して、音楽として外部に出力するための再生処理を説明するフローチャートである。

【００５２】

図３を参照して、携帯電話のキーボード１１０８等からのユーザの指示により、再生リクエストがコントローラ１１０６に与えられる（ステップＳ１００）。

【００５３】

この再生リクエストに応じて、コントローラ１１０６は、メモリ１１０を制御して暗号化コンテンツキー［Ｋｃ］Ｋｐを読み出す（ステップＳ１０２）。

【００５４】

つづいて、復号処理部１５３０は、メモリ１１０から読み出された暗号化コン

テンツキー［Ｋｃ］Ｋｐに対する復号処理を行なう（ステップＳ１０４）。

【００５５】

復号処理部１５３０においてコンテンツキーＫｃを復号抽出可能な場合は（ステップＳ１０６）、処理は次のステップに移行し、一方、復号不能と判断された場合は、処理は終了する（ステップＳ１１０）。

【００５６】

復号処理部１５３０においてコンテンツキーＫｃを復号抽出可能な場合は、コントローラ１１０８は、メモリ１１０を制御して、暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、復号処理部１５２０に与え、復号処理部１５２０は、復号鍵Ｋｃにより復号処理して、平文化したコンテンツデータＤｃを生成して音楽再生部１５０８に与える。音楽再生部１５０８においてコンテンツデータＤｃより再生された音楽信号は、混合部１５１０を経由して、デジタルアナログ変換器１５１２によりアナログ信号に変換されて接続端子１５１４から外部に出力される。

【００５７】

以上のような構成とすることで、再生装置である携帯電話機１００内のメモリ１１０には、暗号化コンテンツデータと暗号化コンテンツキーが保持されているのみであるため、外部からこのメモリ１１０内の記憶内容を仮に読み出したとしても、音楽を再生することはできない。

【００５８】

しかも、メモリ１１０から復号処理部１５２０および１５３０に与えられるデータも、このような暗号化されたデータであるため、データバスＢＳ２上の信号を外部から仮に検出したとしても、音楽を再生することはできない。

【００５９】

さらに、平文化された音楽データが伝達される部分は、上述のとおり、タンパーレジスタンスモジュールで構成されているので、この部分から音楽データを外部に読み出すこともできない構成となっている。

【００６０】

したがって、図２に示した携帯電話機１００の構成により、不正な手続きでコ

ンテンツデータを複製して、再生あるいは配布を行なうことから保護することが可能となる。

【００６１】

［実施の形態２］

図４は、本発明の実施の形態２の携帯電話機２００の構成を説明するための概略ブロック図であり、実施の形態１の図２と対比される図である。

【００６２】

図２に示した携帯電話機１００の構成と、携帯電話機２００の構成が異なる点は、以下のとおりである。

【００６３】

まず、図４においては、携帯電話機２００には、携帯電話機２００により受信された暗号化コンテンツデータを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機２００中の音楽再生モジュール１５００に与えるための着脱可能なメモリカード１２０が装着される構成となっている。これに応じて、携帯電話機２００は、メモリカード１２０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００をさらに備えている。

【００６４】

さらに、携帯電話機２００の構成では、音楽再生モジュール１５００の構成も、携帯電話機１００の構成と異なる。

【００６５】

すなわち、携帯電話機２００の音楽再生モジュール１５００は、メモリカード１２０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するための後に説明するセッションキーＫｓを乱数等により発生するセッションキー発生部１５０２と、セッションキー発生部１５０２により生成されたセッションキーＫｓを暗号化して、データバスＢＳ２に与えるための暗号化処理部１５０４と、データバスＢＳ２によりメモリカード１２０から伝送され、公開暗号化鍵ＫＰｐおよびセッションキーＫｓにより暗号化コンテンツキーＫｃをセッションキーＫｓについて復号して出力する復号

処理部１５０６と、公開暗号化鍵ＫＰｐに対応し、キーＫＰｐで暗号化されたデータを復号可能な秘密復号鍵Ｋｐを保持するＫｐ保持部１５４０と、復号処理部１５０６の出力を受けて、メモリカード１２０から伝送され公開暗号化鍵ＫＰｐにより暗号化コンテンツキー［Ｋｃ］Ｋｐを復号するための復号処理部１５３０と、サーバ３０から配信されメモリカード１２０中に格納された暗号化コンテンツデータ［Ｄｃ］Ｋｃを、復号処理部１５３０で復号抽出されたコンテンツキーＫｃに基づいて復号するための復号処理部１５２０と、復号処理部１５２０からの復号されたコンテンツデータＤｃを受けて、音楽サーバ３０から配信された音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２とを含む。

【００６６】

携帯電話機２００のその他の部分は、実施の形態１の携帯電話機１００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【００６７】

なお、図４においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【００６８】

また、図４に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５０６、暗号化処理部１５０４およびＫｓ発生部１５０２を、ＴＲＭに組み込む構成とすることが可能である。

【００６９】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機２００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【００７０】

さらに、図４において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータついても、保護することが可能である。

【００７１】

［暗号／復号鍵の構成］

図５は、図４に示した携帯電話機２００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【００７２】

まず、図４に示した構成において、メモリカード１２０内のデータ処理を管理するための鍵としては、メモリカードに固有な公開暗号化鍵ＫＰｍと、公開暗号化鍵ＫＰｍにより暗号化されたデータを復号するためのキーＫＰｍとは非対称な秘密復号鍵Ｋｍとがある。

【００７３】

ここで、キーＫＰｍとキーＫｍとが非対称とは、複数の公開暗号化鍵ＫＰｍにより暗号化されたデータが、キーＫＰｍとは異なりＫＰｍからは容易に類推できない復号鍵Ｋｍにより復号できることを意味する。

【００７４】

したがって、メモリカード１２０と携帯電話機２００とのセッションキーの授受にあたっては、後に説明するようにこれら暗号化鍵Ｋｍ、復号鍵ＫＰｍが用いられることになる。

【００７５】

さらに、メモリカード外でのデータの授受における秘密保持のための暗号化鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵をＫＰｐと、音楽再生モジュール管理の鍵として、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、各通信ごとにＫｓ発生器１５０２において生成される共通鍵Ｋｓとが用いられる。

【００７６】

ここで、共通鍵Ｋｓは、たとえば、携帯電話機２００とメモリカード１２０との間のコンテンツデータの授受のためのアクセスが行なわれるごとにＫｓ発生器１５０２において発生する。

【００７７】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ｋｓを「セッションキー」とも呼ぶことにする。

【００７８】

したがって、セッションキーＫｓは各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

【００７９】

さらに、メモリカード１２０に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、このコンテンツキーＫｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

【００８０】

著作権の存在するコンテンツデータＤｃは、上述のとおり、たとえば音楽データであり、このコンテンツデータをコンテンツキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

【００８１】

また、配信サーバ１０から携帯電話機２００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも公開暗号化鍵ＫＰｐにより暗号化されており、メモリカード１２０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｐとして格納されているものとする。

【００８２】

［メモリカードの構成］

図６は、図４に示したメモリカード１２０の構成を説明するための概略ブロック図である。

【００８３】

メモリカード１２０は、メモリインタフェース１２００との間で信号を端子１

２０２を介して授受するデータバスＢＳ３と、公開暗号化鍵ＫＰｍの値を保持し、データバスＢＳ３に公開暗号化鍵ＫＰｍを出力するためのＫＰｍ保持部１４０１と、カード１２０に対応する秘密復号鍵Ｋｍを保持するためのＫｍ保持部１４０２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、秘密復号鍵Ｋｍにより復号処理をすることにより、セッションキーＫｓを抽出する復号処理部１４０４と、データバスＢＳ３から、公開暗号化鍵Ｋｐで暗号化されているコンテンツキーＫｃおよびコンテンツキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納するためのメモリ１４１２と、復号処理部１４０４により抽出されたセッションキーＫｓに基づいて、メモリ１４１２からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４０６と、メモリカード１２０の動作を制御するためのコントローラ１４２０とを備える。

【００８４】

なお、図６のメモリカード１２０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

【００８５】

［再生処理］

図７は、携帯電話機２００内において、メモリカード１２０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【００８６】

図７を参照して、携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストがメモリカード１２０に対して出力される（ステップＳ２００）。

【００８７】

メモリカード１２０においては、この再生リクエストに応じて、コントローラ１４２０は、ＫＰｍ保持部１４０１から、データバスＢＳ３、端子１２０２およ

びメモリインタフェース１２００を介して、公開暗号化鍵ＫＰｍを携帯電話機２００に対して送信する（ステップＳ２０２）。

【００８８】

携帯電話機２００では、カード１２０からのキーＫＰｍを受信すると（ステップＳ２０４）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成し（ステップＳ２０６）、暗号化処理部１５０４が、キーＫＰｍにより、セッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］ＫＰｍを生成し、データバスＢＳ２を介して、カード１２０に対して送信する（ステップＳ２０８）。

【００８９】

メモリカード１２０は、携帯電話機２００により生成された暗号化セッションキー［Ｋｓ］ＫＰｍを受け取り、復号処理部１４０４において秘密復号鍵Ｋｍにより復号し、セッションキーＫｓを抽出する（ステップＳ２１０）。

【００９０】

続いて、メモリカード１２０は、メモリ１４１２から、コンテンツキー［Ｋｃ］Ｋｐを読出す（ステップＳ２１２）。

【００９１】

続いて、メモリカード１２０は、暗号化処理部１４０６において抽出したセッションキーＫｓにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］ＫｓをデータバスＢＳ２に与える（ステップＳ２１４）。

【００９２】

携帯電話機２００の復号処理部１５０６は、メモリカード１２０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］ＫｓをセッションキーＫｓにより復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを取得する（ステップＳ２１６）。

【００９３】

さらに、携帯電話機２００の復号処理部１５３０は、Ｋｐ保持部１５４０からのキーＫｐに基づいて、データ［Ｋｃ］Ｋｐの復号処理を行なう（ステップＳ２１８）。

【００９４】

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は（ステップＳ２２０）、処理は次のステップＳ２２２に進み、抽出できない場合は（ステップＳ２２０）、処理は終了する（ステップＳ２２６）。

【００９５】

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ２に与える（ステップＳ２２２）。

【００９６】

携帯電話機２００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２２６）。

【００９７】

このような構成とすることで、携帯電話機２００において生成されたセッションキーに基づいてコンテンツキーを暗号化した上で、メモリカード１２０から携帯電話機２００に送信して再生動作を行なうことが可能となる。

【００９８】

以上のような構成により、実施の形態１の携帯電話機１００の奏する効果に加えて、実施の形態２の携帯電話機２００においては、携帯電話機２００に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

【００９９】

しかも、携帯電話機とメモリカードとの間のデータの授受は、セッションキーにより暗号化された上で行なわれるので、データに対するセキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

【０１００】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

【０１０１】

［実施の形態３］

図８は、本発明の実施の形態３の携帯電話機３００の構成を説明するための概略ブロック図であり、実施の形態２の図４と対比される図である。

【０１０２】

図８に示した実施の形態３の携帯電話機３００の構成と、実施の形態２の携帯電話機２００の構成が異なる点は、以下のとおりである。

【０１０３】

まず、図８においては、携帯電話機３００には、携帯電話機３００により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機３００中の音楽再生モジュール１５００に与えるための着脱可能なメモリカード１３０が装着される構成となっている。

【０１０４】

メモリカード１３０は、後に説明するように、メモリカード１３０自身でセッションキーＫｓ２を生成する点で、メモリカード１２０と異なる。

【０１０５】

さらに、携帯電話機３００の構成では、音楽再生モジュール１５００の構成も、携帯電話機２００の構成と異なる。

【０１０６】

すなわち、携帯電話機３００の音楽再生モジュール１５００は、メモリカード１３０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ１を乱数等により発生するセッションキー発生部１５５２と、セッションキー発生部１５５２により生成されたセッションキーＫｓ１をメモリカード１３０からのセッショ

ンキーＫｓ２で暗号化して、データバスＢＳ２に与えるための暗号化処理部１５５４と、データバスＢＳ２によりメモリカード１３０から伝送され、公開暗号化鍵ＫＰｐおよびセッションキーＫｓ１により暗号化コンテンツキーＫｃをセッションキーＫｓ１について復号して出力する復号処理部１５５６と、コントローラ１１０６により制御されて、データバスＢＳ２により伝達された暗号化されたメモリカード１３０のセッションキー［Ｋｓ２］Ｋｐまたは復号処理部１５５６から出力された暗号化コンテンツキー［Ｋｃ］Ｋｐのいずれかを、公開暗号化鍵ＫＰｐにより暗号化されたデータを復号するための復号処理部１５３０に与える切換え回路１５５０とを含む。

【０１０７】

暗号化処理部１５５４は、復号処理部１５３０において秘密復号鍵Ｋｐにより復号されて抽出されたメモリカード１３０のセッションキーＫｓ２を受けて、セッションキー発生部１５５２により生成されたセッションキーＫｓ１をセッションキーＫｓ２で暗号化処理する。

【０１０８】

携帯電話機３００のその他の部分は、実施の形態２の携帯電話機２００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１０９】

なお、図８においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【０１１０】

また、図８に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２および切換え回路１５５０を、ＴＲＭに組み込む構成とすることが可能である。

【０１１１】

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機３００の暗号化方式および秘密復号

鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【０１１２】

さらに、図８において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータついても、保護することが可能である。

【０１１３】

［暗号／復号鍵の構成］

図９は、図８に示した携帯電話機３００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【０１１４】

まず、図８に示した構成において、メモリカード１３０内のデータ処理を管理するための鍵としては、メモリカードに固有な公開暗号化鍵ＫＰｍと、公開暗号化鍵ＫＰｍにより暗号化されたデータを復号するためのキーＫＰｍとは非対称な秘密復号鍵Ｋｍと、メモリカード１３０が生成し各セッションに固有なセッションキーＫｓ２とがある。

【０１１５】

したがって、メモリカード１３０と携帯電話機３００とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵Ｋｍ、復号鍵ＫＰｍ、セッションキーＫｓ２が用いられることになる。

【０１１６】

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵であって、コンテンツデータの配信時にコンテンツデータとともに配信され、後に説明するようにメモリカード１３０内に記憶される公開暗号鍵ＫＰｐと、音楽再生モジュールの管理の鍵として、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、各アクセスごとにセッションキー発生器１５５２において生成される共通鍵であるセッションキーＫｓ１とが用いられる。

【０１１７】

セッションキーＫｓ１も各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

【０１１８】

さらに、メモリカード１３０に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、このコンテンツキーＫｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

【０１１９】

また、配信サーバ１０から携帯電話機３００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも公開暗号化鍵ＫＰｐにより暗号化されており、メモリカード１３０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｐとして格納されているものとする。

【０１２０】

さらに、著作権の存在するコンテンツデータＤｃは、このコンテンツデータをコンテンツキーＫｃで復号化可能な暗号化コンテンツデータ［Ｄｃ］Ｋｃとしてメモリカード１３０に格納されているものとする。

【０１２１】

［メモリカードの構成］

図１０は、図８に示したメモリカード１３０の構成を説明するための概略ブロック図である。

【０１２２】

メモリカード１３０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、セッション毎にセッションキーＫｓ２を生成するためのセッションキー発生部１４５０と、セッションキーＫｓ２を公開暗号化鍵ＫＰｐで暗号化してデータバスＢＳ３に与えるための暗号化処理部１４５２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータ［Ｋｓ１］Ｋｓ２から、セッションキーＫｓ２により復号処理をすることにより、携帯電話機３００からのセッションキーＫｓ１を抽出する復号処理部１４５４と、データバスＢＳ３から、公開暗号化鍵ＫＰｐと、公開暗号化鍵ＫＰ

ｐで暗号化されているコンテンツキー［Ｋｃ］Ｋｐとコンテンツキー Ｋｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃとの３つを受けて格納するためのメモリ１４１２と、復号処理部１４５４により抽出されたセッションキーＫｓ１に基づいて、メモリ１４１２からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４５６と、メモリカード１３０の動作を制御するためのコントローラ１４２０とを備える。

【０１２３】

なお、図１０のメモリカード１３０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

【０１２４】

［再生処理］

図１１は、携帯電話機３００内において、メモリカード１３０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【０１２５】

図１１を参照して、携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストがメモリカード１３０に対して出力される（ステップＳ３００）。

【０１２６】

メモリカード１３０においては、この再生リクエストに応じて、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ３０２）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機３００に対して送信する（ステップＳ３０４）。

【０１２７】

携帯電話機３００では、カード１３０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ３０６）。

【０１２８】

携帯電話機３００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ３０８）、暗号化処理部１５５４が、ステップＳ３０６において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化して暗号化セッションキー［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１３０に対して送信する（ステップＳ３１０）。

【０１２９】

メモリカード１３０は、携帯電話機３００により生成され、かつ暗号化されたセッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ３１２）。

【０１３０】

続いて、メモリカード１３０は、メモリ１４１２から、暗号化コンテンツキー［Ｋｃ］Ｋｐを読出し（ステップＳ３１４）、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ３１６）。

【０１３１】

携帯電話機３００の復号処理部１５５６は、メモリカード１３０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１に対してセッションキーＫｓ１により復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｐを取得する（ステップＳ３１８）。

【０１３２】

さらに、携帯電話機３００の復号処理部１５３０は、切換え回路１５５０を介

して暗号化コンテンツキー［Ｋｃ］Ｋｐを受け、Ｋｐ保持部１５４０からのキーＫｐに基づいて、暗号化コンテンツキー［Ｋｃ］Ｋｐの復号処理を行なう（ステップＳ３２０）。

【０１３３】

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は（ステップＳ３２２）、処理は次のステップＳ３２４に進み、抽出できない場合は（ステップＳ３２２）、処理は終了する（ステップＳ３３０）。

【０１３４】

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１３０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ３２４）。

【０１３５】

携帯電話機３００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し（ステップＳ３２８）、処理が終了する（ステップＳ３３０）。

【０１３６】

このような構成とすることで、携帯電話機３００において生成されたセッションキーＫｓ１に基づいて暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化した上で、メモリカード１３０から携帯電話機３００に送信して再生動作を行なうことが可能となる。しかも、メモリカード１３０においてセッション毎に生成されたセッションキーＫｓ２により暗号化した上で、メモリカード１３０と携帯電話機３００との間でセッションキーＫｓ１の授受が行なわれるので、実施の形態２よりも一層、セキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

【０１３７】

また、以上のような構成により、実施の形態３の携帯電話機３００においても、携帯電話機３００に対して、着脱可能なメモリカード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

【０１３８】

さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

【０１３９】

［実施の形態４］

図１２は、本発明の実施の形態４の携帯電話機４００の構成を説明するための概略ブロック図であり、実施の形態３の図８と対比される図である。

【０１４０】

図１２に示した実施の形態４の携帯電話機４００の構成と、実施の形態３の携帯電話機３００の構成が異なる点は、以下のとおりである。

【０１４１】

すなわち、図１２においては、携帯電話機４００には、携帯電話機４００により受信された暗号化コンテンツデータおよび暗号化コンテンツキーを受取って格納し、さらに所定の暗号化処理をした上で、携帯電話機４００中の音楽再生モジュール１５００に与えるための着脱可能なメモリカード１４０が装着される構成となっている。メモリカード１４０は、後に説明するように、携帯電話機４００に対する認証機能を有する点で実施の形態３のメモリカード１３０と異なる。

【０１４２】

さらに、携帯電話機４００の構成では、音楽再生モジュール１５００の構成も、携帯電話機３００の構成と異なる。

【０１４３】

すなわち、携帯電話機４００の音楽再生モジュール１５００は、メモリカード１４０と携帯電話の他の部分とのデータ授受にあたり、携帯電話機４００に対す

る認証機能を実現するために、再生装置である携帯電話機４００のクラス（種類等）に固有な公開暗号鍵ＫＰｐと認証データＣｒｔｆとを、システムに共通な公開復号鍵（公開認証鍵）ＫＰｍａにより暗号化して保持する［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０をさらに備える構成となっている点である。

【０１４４】

携帯電話機４００のその他の部分は、実施の形態３の携帯電話機３００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１４５】

なお、図１２においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【０１４６】

また、図１２に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２、切換え回路１５５０および［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０を、ＴＲＭに組み込む構成とすることが可能である。

【０１４７】

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機４００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【０１４８】

さらに、図１２において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータついても、保護することが可能である。

【０１４９】

［暗号／復号鍵の構成］

図１３は、図１２に示した携帯電話機４００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【０１５０】

まず、図１２に示した構成において、メモリカード１４０内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵であり、認証鍵の機能を有するＫＰｍａと、メモリカード１４０が生成し各セッションに固有な共通鍵であるセッションキーＫｓ２とがある。

【０１５１】

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のクラスに固有な公開暗号化鍵であって、上述のとおり、鍵ＫＰｍａにより暗号化された形で携帯電話機４００中の［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０に格納されている公開暗号鍵ＫＰｐと、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、各アクセスごとにセッションキー発生器１５５２において生成される共通鍵でるセッションキーＫｓ１とが用いられる。

【０１５２】

セッションキーＫｓ１も各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

【０１５３】

なお、「再生装置のクラス」とは、再生装置ごと、あるいは、再生装置の種類（製造メーカ、製造ロット）ごとに、この再生装置を区別するための区分であるものとする。

【０１５４】

さらに、メモリカード１４０に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、このコンテンツキーＫｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

【０１５５】

また、配信サーバ１０から携帯電話機４００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも公開暗号化鍵ＫＰｐにより暗号化されており、メモリカード１４０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｐとして格納されているものとする。

【０１５６】

さらに、著作権の存在するコンテンツデータＤｃは、このコンテンツデータをコンテンツキーＫｃで復号化可能な暗号化コンテンツデータ［Ｄｃ］Ｋｃとしてメモリカード１４０に格納されているものとする。

【０１５７】

［メモリカードの構成］

図１４は、図１２に示したメモリカード１４０の構成を説明するための概略ブロック図である。

【０１５８】

メモリカード１４０の構成が、実施の形態３のメモリカード１３０の構成と異なる点は、まず、コントローラ１４２０に制御されて、データバスＢＳ３上のデータに対して公開復号鍵ＫＰｍａによる復号処理を行い、携帯電話機１４０からの公開暗号鍵ＫＰｐおよび認証データＣｒｔｆの取得を行うための復号処理部１４６０を備える構成となっている点である。したがって、暗号化処理部１４５２は、復号処理部１４６０からの公開暗号化鍵ＫＰｐに基づいて暗号化処理を行う。

【０１５９】

さらに、メモリカード１４０中のメモリ１４１２においては、メモリカード１３０の場合に保持されていた公開暗号化鍵ＫＰｐの代わりに、公開復号鍵ＫＰｍａが格納されている。したがって、復号処理部１４６０は、メモリ１４１２中に保持された公開復号鍵ＫＰｍａに基づいて復号処理を行う。

【０１６０】

メモリカード１４０のその他の部分は、実施の形態３のメモリカード１３０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１６１】

なお、図１４のメモリカード１４０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内の鍵等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

【０１６２】

［再生処理］

図１５は、携帯電話機４００内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

【０１６３】

図１５を参照して、再生処理の説明を行なう。携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストが与えられると（ステップＳ４００）、携帯電話機４００の［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａ保持部１５６０からメモリカード１４０に対してデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａが出力される（ステップＳ４０２）。

【０１６４】

メモリカード１４０においては、このデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａを復号部１４６０により復号し、公開暗号化鍵ＫＰｐと認証データＣｒｔｆとを獲得する（ステップＳ４０６）。コントローラ１４２０は、認証データＣｒｔｆに基づいて携帯電話機４００の認証を行ない（ステップＳ４０６）、携帯電話機４００が正規の機器であれば処理をステップＳ４０８に移行し、携帯電話機４００が正規の機器でない場合、再生のための動作を行なわずに処理を終了する（ステップＳ４３４）。

【０１６５】

携帯電話機４００が正規の機器である場合、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ４０８）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッショ

ンキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機４００に対して送信する（ステップＳ４１０）。

【０１６６】

携帯電話機４００では、カード１４０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ４１２）。

【０１６７】

携帯電話機４００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ４１４）、暗号化処理部１５５４が、ステップＳ４１２において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化してデータ［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１４０に対して送信する（ステップＳ４１６）。

【０１６８】

メモリカード１４０は、携帯電話機４００により生成され、かつ暗号化されたセッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ４１８）。

【０１６９】

続いて、メモリカード１４０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ］Ｋｐを読出し（ステップＳ４２０）、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、暗号化コンテンツキー［Ｋｃ］Ｋｐを暗号化し、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ４２２）。

【０１７０】

携帯電話機４００の復号処理部１５５６は、メモリカード１４０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｐ］Ｋｓ１に対してセッションキーＫｓ１により復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ

］Ｋｐを取得する（ステップＳ４２４）。

【０１７１】

さらに、携帯電話機４００の復号処理部１５３０は、切換え回路１５５０を介して暗号化コンテンツキー［Ｋｃ］Ｋｐを受け、Ｋｐ保持部１５４０からのキーＫｐに基づいて、データ［Ｋｃ］Ｋｐの復号処理を行なう（ステップＳ４２６）。

【０１７２】

復号処理部１５３０が、復号処理によりコンテンツキーＫｃを抽出できた場合は（ステップＳ４２８）、処理は次のステップＳ４３０に進み、抽出できない場合は（ステップＳ４２８）、処理は終了する（ステップＳ４３４）。

【０１７３】

復号処理部１５３０が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ４３０）。

【０１７４】

携帯電話機４００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文の音楽データＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップＳ４３２）、処理が終了する（ステップＳ４３４）。

【０１７５】

このような構成とすることで、実施の形態３の携帯電話機３００およびメモリカード１３０の奏する効果に加えて、携帯電話機４００からのデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａに基づいて、メモリカード１４０が認証の結果、正規の機器と判断された携帯電話機４００とメモリカード１４０の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

【０１７６】

［実施の形態５］

図１６は、本発明の実施の形態５の携帯電話機５００の構成を説明するための概略ブロック図であり、実施の形態４の図１２と対比される図である。

【０１７７】

図１６に示した実施の形態５の携帯電話機５００の構成と、実施の形態４の携帯電話機４００の構成が異なる点は、以下のとおりである。

【０１７８】

すなわち、図１６においては、メモリカード１４０に代わりメモリカード１５０が装着されており、さらに、メモリカード１５０から携帯電話機５００に対してコンテンツキーＫｃを送信する場合は、セッションキーＫｓ１により暗号化されたデータ［Ｋｃ］Ｋｓ１として送信される。したがって、実施の形態４の場合のように、コンテンツキーＫｃの送信の際に、キーＫＰｐとキーＫｓ１により２重に暗号化されているわけではないため、キーＫｓ１による復号処理とキーＫｐによる復号処理とは、独立に行なうことが可能となり、図１６に示した携帯電話機５００においてはにおいては切換スイッチ１５５０が省略されている。

【０１７９】

すなわち、携帯電話機５００の音楽再生モジュール１５００は、秘密復号鍵Ｋｐを保持するためのＫｐ保持部１５４０と、メモリカード１５０からデータバスＢｓ２を介して与えられるデータ［Ｋｓ２］ＫｐをキーＫｐにより復号化するための復号処理部１５３０と、メモリカード１５０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ１を乱数等により発生するセッションキー発生部１５５２と、セッションキー発生部１５５２により生成されたセッションキーＫｓ１をメモリカード１５０からのセッションキーＫｓ２で暗号化して、データバスＢＳ２に与えるための暗号化処理部１５５４と、データバスＢＳ２によりメモリカード１５０から伝送され、セッションキーＫｓ１により暗号化コンテンツキーＫｃをセッションキーＫｓ１について復号して出力する復号処理部１５５６と、復号処理部１５５６から出力されるコンテンツキーＫｃに基づいて、データバ

スＢｓ２を介してメモリカード１５０から与えられる暗号化コンテンツデータ［Ｄｃ］Ｋｃを復号して音楽再生部１５０８に与えるための復号処理部１５２０と、メモリカード１５０と携帯電話の他の部分とのデータ授受にあたり、携帯電話機５００に対する認証機能を実現するために、再生装置である携帯電話機５００のクラス（種類等）に固有な公開暗号鍵ＫＰｐと認証データＣｒｔｆとを、システムに共通な公開復号鍵ＫＰｍａにより暗号化して保持する［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０とを備える。

【０１８０】

携帯電話機５００のその他の部分は、実施の形態４の携帯電話機４００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１８１】

なお、図１６においても、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【０１８２】

また、図１６に示した構成においても、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２および［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０を、ＴＲＭに組み込む構成とすることが可能である。

【０１８３】

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機５００の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

【０１８４】

さらに、図１６において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータついても、保護することが可能である。

【０１８５】

［メモリカードの構成］

図１７は、図１６に示したメモリカード１５０の構成を説明するための概略ブロック図である。

【０１８６】

メモリカード１５０の構成が、実施の形態４のメモリカード１４０の構成と異なる点は、コンテンツキーＫｃがメモリ１４１２中に暗号化されることなく、平分データとして格納されている点である。

【０１８７】

メモリカード１５０のその他の部分は、実施の形態４のメモリカード１４０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１８８】

なお、図１７のメモリカード１５０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とする。

【０１８９】

［再生処理］

図１８は、携帯電話機５００内において、メモリカード１５０に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【０１９０】

図１８を参照して、再生処理についての説明を行なう。携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストが与えられると（ステップＳ５００）、携帯電話機５００の［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａ保持部１５６０からメモリカード１５０に対してデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａが出力される（ステップＳ５０２）。

【０１９１】

メモリカード１５０においては、このデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａを復号部１４６０により復号し、公開暗号化鍵ＫＰｐと認証データＣｒｔｆとを獲得する（ステップＳ５０６）。コントローラ１４２０は、認証データＣｒｔｆに基づいて携帯電話機５００の認証を行ない（ステップＳ５０６）、携帯電話機５００が正規の機器であれば処理をステップＳ５０８に移行し、携帯電話機５００が正規の機器でない場合、再生のための動作を行なわずに処理を終了する（ステップＳ５３４）。

【０１９２】

携帯電話機５００が正規の機器である場合、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ５０８）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機５００に対して送信する（ステップＳ５１０）。

【０１９３】

携帯電話機５００では、カード１５０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ５１２）。

【０１９４】

携帯電話機５００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ５１４）、暗号化処理部１５５４が、ステップＳ５１２において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化してデータ［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１５０に対して送信する（ステップＳ５１６）。

【０１９５】

メモリカード１５０は、携帯電話機５００により生成され、かつ暗号化されたセッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッ

ションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ５１８）。

【０１９６】

続いて、メモリカード１５０は、メモリ１４１２から、コンテンツキーＫｃを読出す（ステップＳ５２０）。

【０１９７】

続いて、メモリカード１５０は、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、コンテンツキーＫｃを暗号化し、暗号化コンテンツキー［Ｋｃ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ５２２）。

【０１９８】

携帯電話機５００の復号処理部１５５６は、メモリカード１５０から送信された暗号化された暗号化コンテンツキー［Ｋｃ］Ｋｓ１に対して、セッションキーＫｓ１により復号処理を行なうことにより、コンテンツキーＫｃを取得する（ステップＳ５２４）。

【０１９９】

メモリカード１５０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ５３０）。

【０２００】

携帯電話機５００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し（ステップＳ５３２）、処理が終了する（ステップＳ５３４）。

【０２０１】

このような構成とすることで、実施の形態４の携帯電話機４００およびメモリカード１３０の奏する効果と同様に、携帯電話機５００からのデータ［ＫＰｐ，

Ｃｒｔｆ］ＫＰｍａに基づいて、メモリカード１５０が認証の結果、正規の機器と判断された携帯電話機５００とメモリカード１５０の間でしか再生動作が行なわれないため、著作権者の著作権の保護を図ることが、より簡易な構成で可能となる。

【０２０２】

［実施の形態６］

図１９は、本発明の実施の形態６の携帯電話機６００の構成を説明するための概略ブロック図であり、実施の形態５の図１６と対比される図である。

【０２０３】

図１９に示した実施の形態６の携帯電話機６００の構成と、実施の形態５の携帯電話機５００の構成が異なる点は、以下のとおりである。

【０２０４】

すなわち、図１９においては、携帯電話機６００は、システム共通の秘密復号鍵Ｋｃｏｍを保持するためのＫｃｏｍ保持部１５７０と、復号処理部１５５６の出力を受けて、秘密復号鍵Ｋｃｏｍにより復号してコンテンツキーＫｃを獲得し、復号処理部１５２０に与える復号処理部１５７２をさらに備える構成となっている。

【０２０５】

すなわち、実施の形態５においては、メモリカード１５０から携帯電話機５００に対してコンテンツキーＫｃを送信する場合は、セッションキーＫｓ１により暗号化されたコンテンツキー［Ｋｃ］Ｋｓ１として送信されたのに対し、実施の形態６においては、メモリカード１６０から携帯電話機６００に対してコンテンツキーＫｃを送信する場合は、秘密復号鍵Ｋｃｏｍおよびセッションキー Ｋｓ１により復号可能なように暗号化されたコンテンツキー［［Ｋｃ］Ｋｃｏｍ］Ｋｓ１として送信される。

【０２０６】

携帯電話機６００のその他の部分は、実施の形態５の携帯電話機５００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０２０７】

なお、図１９においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【０２０８】

また、図１９に示した構成において、音楽再生部１５０８、Ｋｐ保持部１５４０、復号処理部１５３０、復号処理部１５２０、復号処理部１５５６、暗号化処理部１５５４、セッションキー発生部１５５２、［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０、Ｋｃｏｍ保持部および復号処理部１５７２を、ＴＲＭに組み込む構成とすることが可能である。

【０２０９】

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたコンテンツデータを外部から不正に取得することができなくなり、セキュリティが向上する。

【０２１０】

さらに、図１９において実線で囲んだ領域に相当する音楽再生モジュール１５００を、ＴＲＭとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータついても、保護することが可能である。

【０２１１】

［暗号／復号鍵の構成］

図２０は、図１９に示した携帯電話機６００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【０２１２】

まず、図１９に示した構成において、メモリカード１６０内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵ＫＰｍａと、メモリカード１６０が生成し各セッションに固有なセッションキーＫｓ２とがある。

【０２１３】

さらに、メモリカード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のク

ラスに固有な公開暗号化鍵であって、鍵ＫＰｍａにより暗号化された形で携帯電話機６００中の［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部１５６０に格納されている公開暗号鍵ＫＰｐと、このキーＫＰｐで暗号化されたデータを復号化でき、キーＫＰｐとは非対称な秘密復号鍵Ｋｐと、システムに共通な秘密復号鍵Ｋｃｏｍと、各アクセスごとにセッションキー発生器１５５２において生成される共通鍵であるセッションキーＫｓ１とが用いられる。

【０２１４】

セッションキーＫｓ１も各通信セッションに固有の値を有することになり、音楽再生モジュール１５００において管理される。

【０２１５】

さらに、メモリカード１６０に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツキーＫｃがあり、この共通鍵Ｋｃにより暗号化コンテンツデータが復号（平文化）されるものとする。

【０２１６】

また、配信サーバ１０から携帯電話機６００に向けて、コンテンツキーＫｃが配信される場合には、このコンテンツキーＫｃは、すくなくとも秘密復号鍵Ｋｃｏｍにより復号可能なように暗号化されており、メモリカード１６０中には、この暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍとして格納されているものとする。

【０２１７】

さらに、著作権の存在するコンテンツデータＤｃは、このコンテンツデータをコンテンツキーＫｃで復号化可能な暗号化コンテンツデータ［Ｄｃ］Ｋｃとしてメモリカード１６０に格納されているものとする。

【０２１８】

［メモリカードの構成］

図２１は、図１９に示したメモリカード１６０の構成を説明するための概略ブロック図である。

【０２１９】

メモリカード１６０の構成が、実施の形態５のメモリカード１５０の構成と異

なる点は、コンテンツキーＫｃがメモリ１４１２中においては、暗号化データ［Ｋｃ］Ｋｃｏｍとして格納されている点である。

【０２２０】

メモリカード１６０のその他の部分は、実施の形態５のメモリカード１５０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０２２１】

なお、図２１のメモリカード１６０内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれる構成とすることも可能である。

【０２２２】

［再生処理］

図２２は、携帯電話機６００内において、メモリカード１６０に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

【０２２３】

図２２を参照して、携帯電話機のキーボード１１０８等からのユーザの指示により、再生リクエストが与えられると（ステップＳ６００）、携帯電話機６００の［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａ保持部１５６０からメモリカード１６０に対してデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａが出力される（ステップＳ６０２）。

【０２２４】

メモリカード１６０においては、このデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａを復号部１４６０により復号し、公開暗号化鍵ＫＰｐと認証データＣｒｔｆとを獲得する（ステップＳ６０６）。コントローラ１４２０は、認証データＣｒｔｆに基づいて携帯電話機６００の認証を行ない（ステップＳ６０６）、携帯電話機６００が正規の機器であれば処理をステップＳ６０８に移行し、携帯電話機６００が正規の機器でない場合、再生のための動作を行なわずに処理を終了する（ステップＳ６３４）。

【０２２５】

携帯電話機６００が正規の機器である場合、コントローラ１４２０は、セッションキー発生部１４５０を制御してセッションキーＫｓ２を発生させる（ステップＳ６０８）。コントローラ１４２０の制御により、このセッションキーＫｓ２を暗号化処理部１４５２は公開暗号化鍵ＫＰｐにより暗号化して暗号化セッションキー［Ｋｓ２］Ｋｐを生成し、この暗号化セッションキー［Ｋｓ２］Ｋｐを、データバスＢＳ３、端子１２０２およびメモリインタフェース１２００を介して、携帯電話機６００に対して送信する（ステップＳ６１０）。

【０２２６】

携帯電話機６００では、カード１６０からの暗号化セッションキー［Ｋｓ２］Ｋｐを受信すると、切換え回路１５５０を介して復号処理部１５３０が暗号化セッションキー［Ｋｓ２］Ｋｐを受けて復号しセッションキーＫｓ２を獲得する（ステップＳ６１２）。

【０２２７】

携帯電話機６００においては、セッションキー発生部１５５２においてセッションキーＫｓ１を生成し（ステップＳ６１４）、暗号化処理部１５５４が、ステップＳ６１２において抽出されたセッションキーＫｓ２により、セッションキーＫｓ１を暗号化して暗号化セッションキー［Ｋｓ１］Ｋｓ２を生成し、データバスＢＳ２を介して、カード１６０に対して送信する（ステップＳ６１６）。

【０２２８】

メモリカード１６０は、携帯電話機６００により生成された暗号化セッションキー［Ｋｓ１］Ｋｓ２を受け取り、復号処理部１４５４においてセッションキーＫｓ２により復号し、セッションキーＫｓ１を抽出する（ステップＳ６１８）。

【０２２９】

続いて、メモリカード１６０は、メモリ１４１２から、暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを読出す（ステップＳ６２０）。

【０２３０】

続いて、メモリカード１６０は、暗号化処理部１４５６において、抽出したセッションキーＫｓ１により、暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを暗号化し

、暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｃｏｍ］Ｋｓ１をデータバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ６２２）。

【０２３１】

携帯電話機６００の復号処理部１５５６は、メモリカード１６０から送信された暗号化された暗号化コンテンツキー［［Ｋｃ］Ｋｃｏｍ］Ｋｓ１に対してセッションキーＫｓ１により復号処理を行なうことにより、暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを取得する（ステップＳ６２４）。

【０２３２】

さらに、携帯電話機６００の復号処理部１５７２は、復号処理部１５５６から暗号化コンテンツキー［Ｋｃ］Ｋｃｏｍを受け、Ｋｃｏｍ保持部１５７０からのキーＫｃｏｍに基づいて、データ［Ｋｃ］Ｋｃｏｍの復号処理を行なう（ステップＳ６２６）。

【０２３３】

復号処理部１５７２が、復号処理によりコンテンツキーＫｃを抽出できた場合は（ステップＳ６２８）、処理は次のステップＳ６３０に進み、抽出できない場合は（ステップＳ６２８）、処理は終了する（ステップＳ６３４）。

【０２３４】

復号処理部１５７２が復号処理により、コンテンツキーＫｃを抽出できた場合は、メモリカード１６０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読出し、データバスＢＳ３等を介してデータバスＢＳ２に与える（ステップＳ６３０）。

【０２３５】

携帯電話機６００の復号処理部１５２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたコンテンツキーＫｃにより復号処理して平文のコンテンツデータＤｃを生成し、音楽再生部１５０８は、コンテンツデータＤｃを再生して混合部１５１０に与える。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップＳ６３２）、処理が終了する（ステップＳ６３４）。

【０２３６】

このような構成とすることで、実施の形態４の携帯電話機４００およびメモリカード１４０の奏する効果と同様に、携帯電話機６００からのデータ［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａに基づいて、メモリカード１６０が認証の結果、正規の機器と判断された携帯電話機６００とメモリカード１６０の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

【０２３７】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０２３８】

【発明の効果】

以上説明したとおり、本願発明にかかるデータ再生装置では、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

【図面の簡単な説明】

【図１】　本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【図２】　図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【図３】　携帯電話機１００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

【図４】　本発明の実施の形態２の携帯電話機２００の構成を説明するための概略ブロック図である。

【図５】　図４に示した携帯電話機２００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図６】　図４に示したメモリカード１２０の構成を説明するための概略ブロック図である。

【図７】　携帯電話機２００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

【図８】　本発明の実施の形態３の携帯電話機３００の構成を説明するための概略ブロック図である。

【図９】　図８に示した携帯電話機３００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図１０】　図８に示したメモリカード１３０の構成を説明するための概略ブロック図である。

【図１１】　携帯電話機３００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

【図１２】　本発明の実施の形態４の携帯電話機４００の構成を説明するための概略ブロック図である。

【図１３】　図１２に示した携帯電話機４００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図１４】　図１２に示したメモリカード１４０の構成を説明するための概略ブロック図である。

【図１５】　メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図１６】　本発明の実施の形態５の携帯電話機５００の構成を説明するための概略ブロック図である。

【図１７】　図１６に示したメモリカード１５０の構成を説明するための概略ブロック図である。

【図１８】　メモリカード１５０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図１９】　本発明の実施の形態６の携帯電話機６００の構成を説明するための概略ブロック図である。

【図２０】　図１９に示した携帯電話機６００において使用される通信のた

めのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図２１】　図１９に示したメモリカード１６０の構成を説明するための概略ブロック図である。

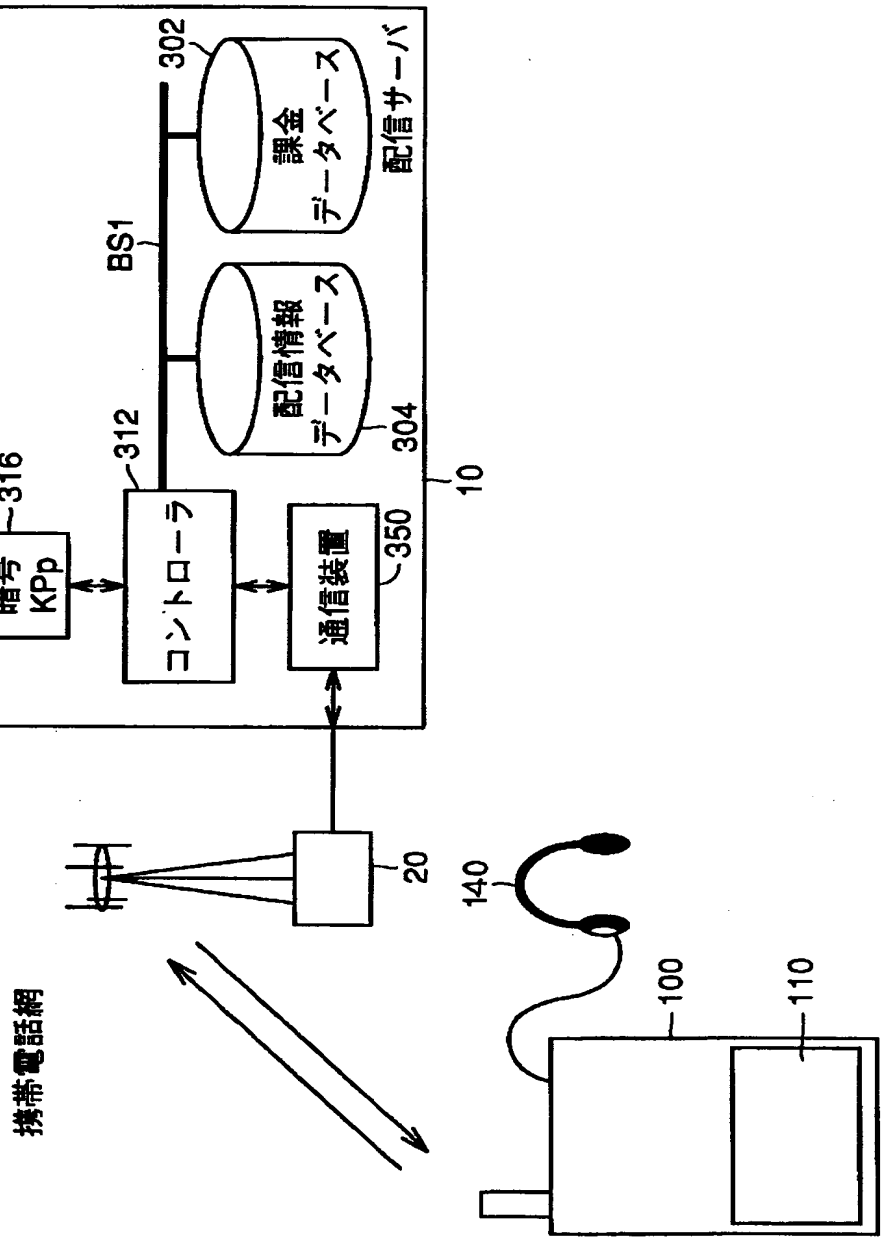
【図２２】　メモリカード１６０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

【符号の説明】

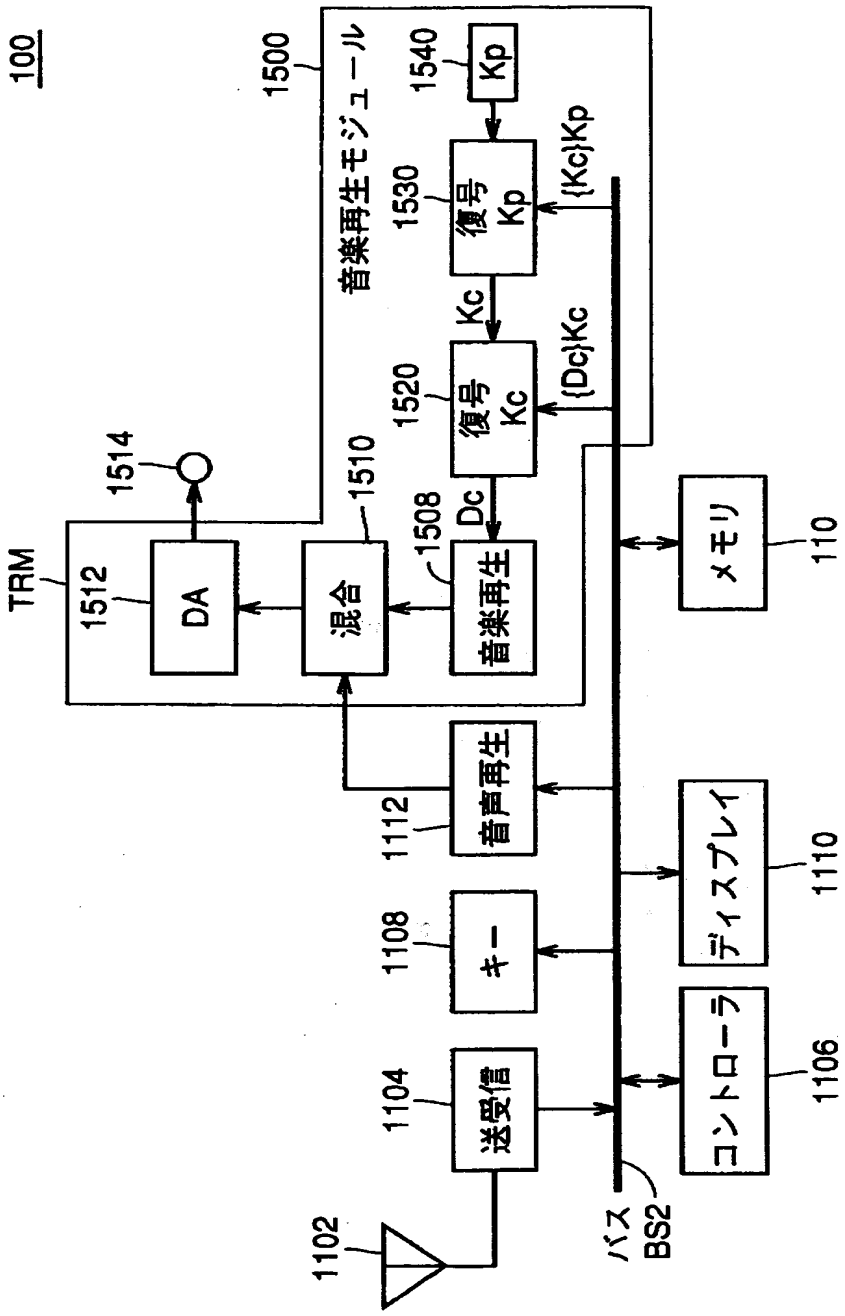
１０　配信サーバ、２０　配信キャリア、３０　音楽サーバ、１００，２００，３００，４００，５００，６００　携帯電話機、１１０，１２０，１３０，１４０，１５０，１６０　メモリカード、１４０　ヘッドホン、１１０２　アンテナ、１１０４　送受信部、１１０６　コントローラ、１１０８　キーボード、１１１０　ディスプレイ、１１１２　音声再生部、１２００　メモリインタフェース、１４０１　ＫＰｍ保持部、１４０４　復号処理部、１４０６　暗号化処理部、１４２０　コントローラ、１５０２　セッションキー発生部、１５０４　暗号化処理部、１５０６　復号処理部、１５０８　音楽再生部、１５１０　混合部、１５１２　デジタルアナログ変換部、１５２０，１５３０　復号処理部、１５４０　Ｋｐ保持部、１５５０　切換え回路、１５６０　［ＫＰｐ、Ｃｒｔｆ］ＫＰｍａ保持部、１５７０　Ｋｃｏｍ保持部、１５７２　復号処理部。

【書類名】　図面

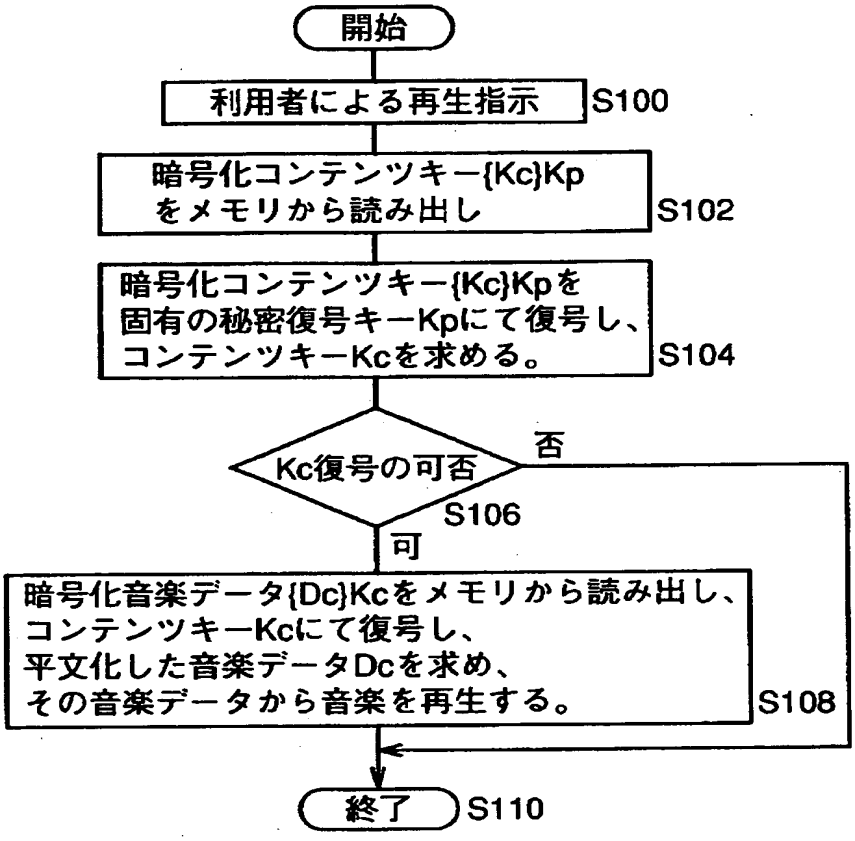
【図１】


302
課金
データベース
配信サーバ
BS1
配信情報
データベース
304
312
316
暗号
KPp
コントローラ
通信装置
350
10
20
140
100
110
携帯電話網

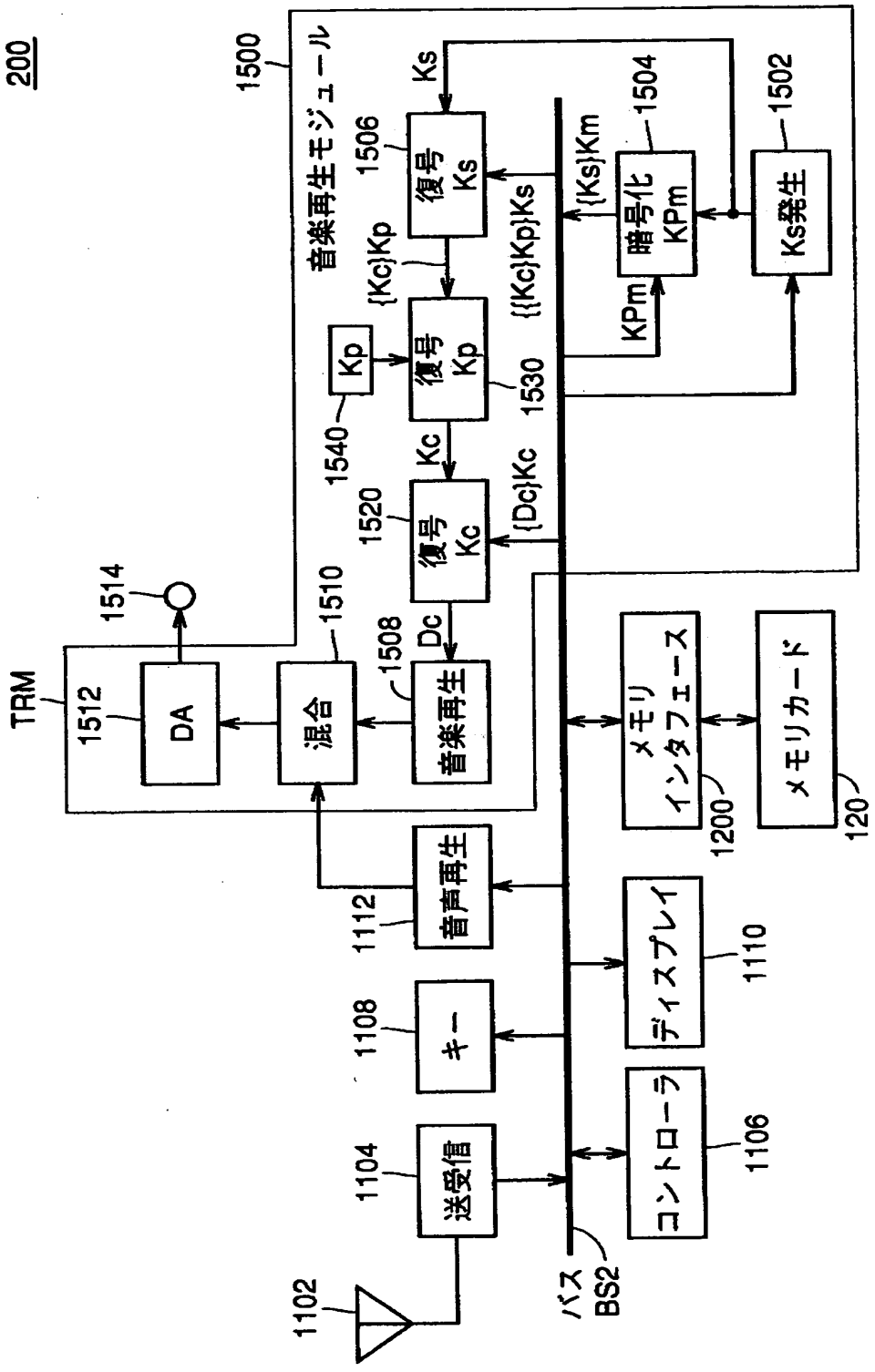
【図２】


100
1500
音楽再生モジュール
1540
Kp
1530
復号
Kp
{Kc}Kp
Kc
1520
復号
Kc
{Dc}Kc
Dc
1508
音楽再生
1510
混合
1514
TRM
1512
DA
メモリ
110
音声再生
1112
ディスプレイ
1110
キー
1108
コントローラ
1106
送受信
1104
1102
バス
BS2

【図３】


開始
利用者による再生指示
S100
暗号化コンテンツキー{Kc}Kp
をメモリから読み出し
S102
暗号化コンテンツキー{Kc}Kpを
固有の秘密復号キーKpにて復号し、
コンテンツキーKcを求める。
S104
Kc復号の可否
S106
否
可
暗号化音楽データ{Dc}Kcをメモリから読み出し、
コンテンツキーKcにて復号し、
平文化した音楽データDcを求め、
その音楽データから音楽を再生する。
S108
終了
S110

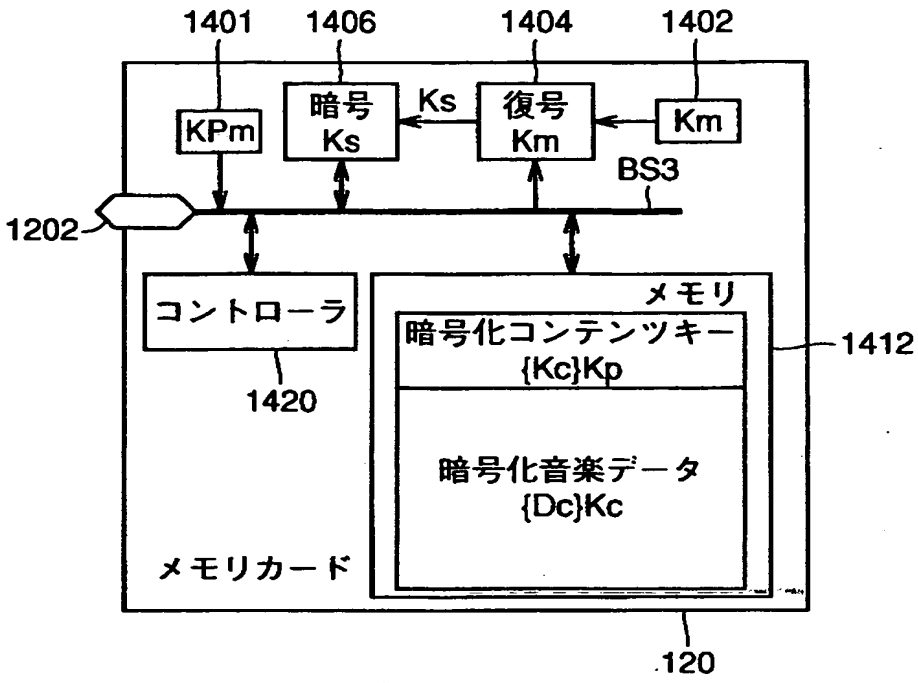
【図４】


200
1500
音楽再生モジュール
Ks
1506
復号 Ks
{Kc}Kp
Kp
1540
復号 Kp
1530
Kc
1520
復号 Kc
{Dc}Kc
Dc
1508
音楽再生
1510
混合
1514
TRM
1512
DA
{Ks}Km
1504
暗号化 KPm
KPm
{{Kc}Kp}Ks
1502
Ks発生
メモリインタフェース
1200
メモリカード
120
音声再生
1112
ディスプレイ
1110
キー
1108
コントローラ
1106
送受信
1104
1102
バス BS2

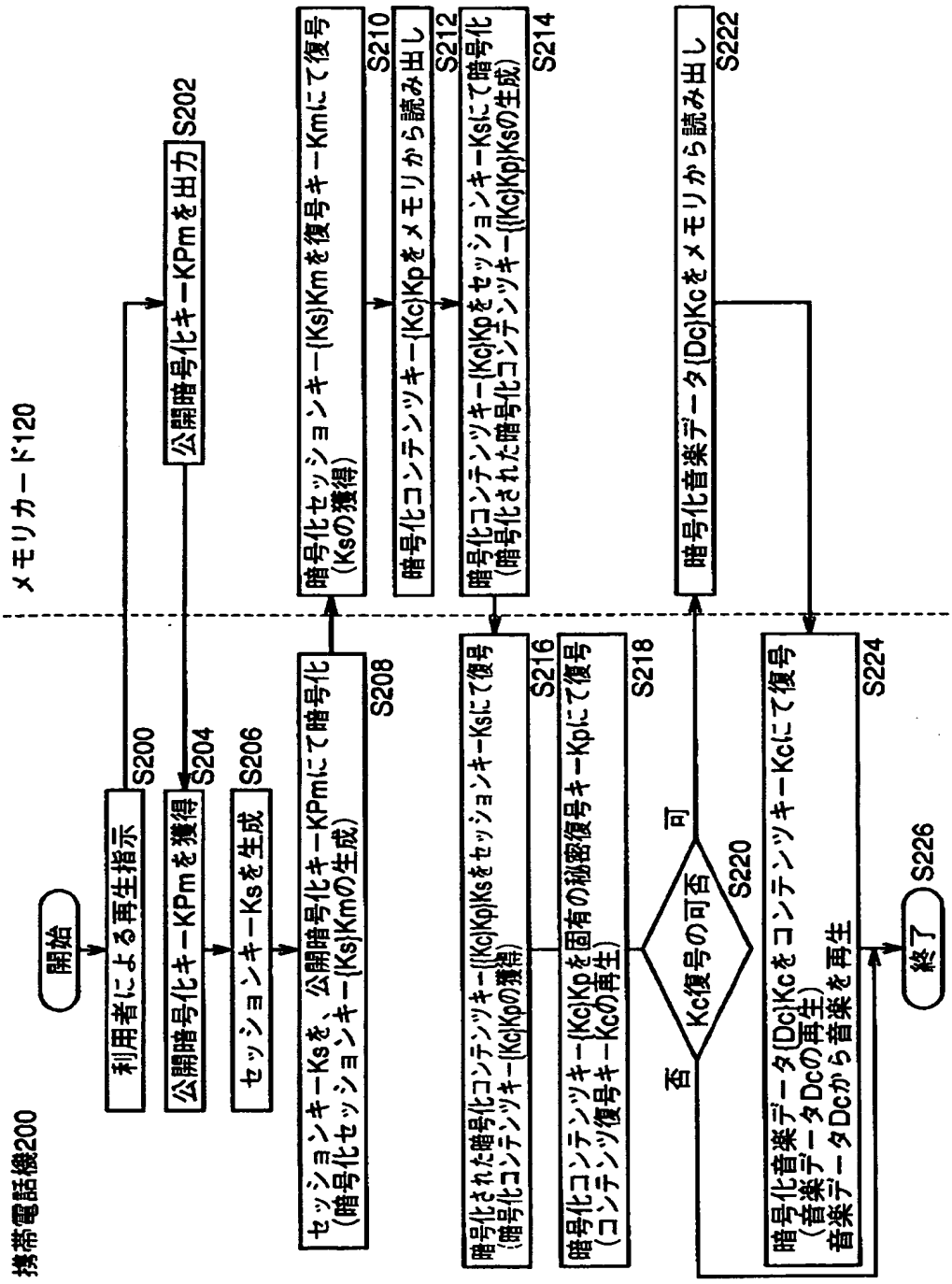
【図５】

	記号	属性	特性	
メモリカード管理の鍵	Km	秘密復号鍵		メモリカード毎に異なる
	KPm	公開暗号鍵	Kmと対を成す	KPmで暗号化されたデータは非対称な復号鍵Kmで復号可能
音楽再生モジュール管理の鍵	Kp	秘密復号鍵	データ再生装置（携帯電話機）固有	データ再生装置毎に異なる
	Ks	共通鍵	セッション固有	メモリと音楽再生モジュール間のアクセス毎に発生
配信データ	KPp	公開暗号鍵	Kpと対を成す（Kcを暗号化）	KPpで暗号化されたデータは非対称な復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

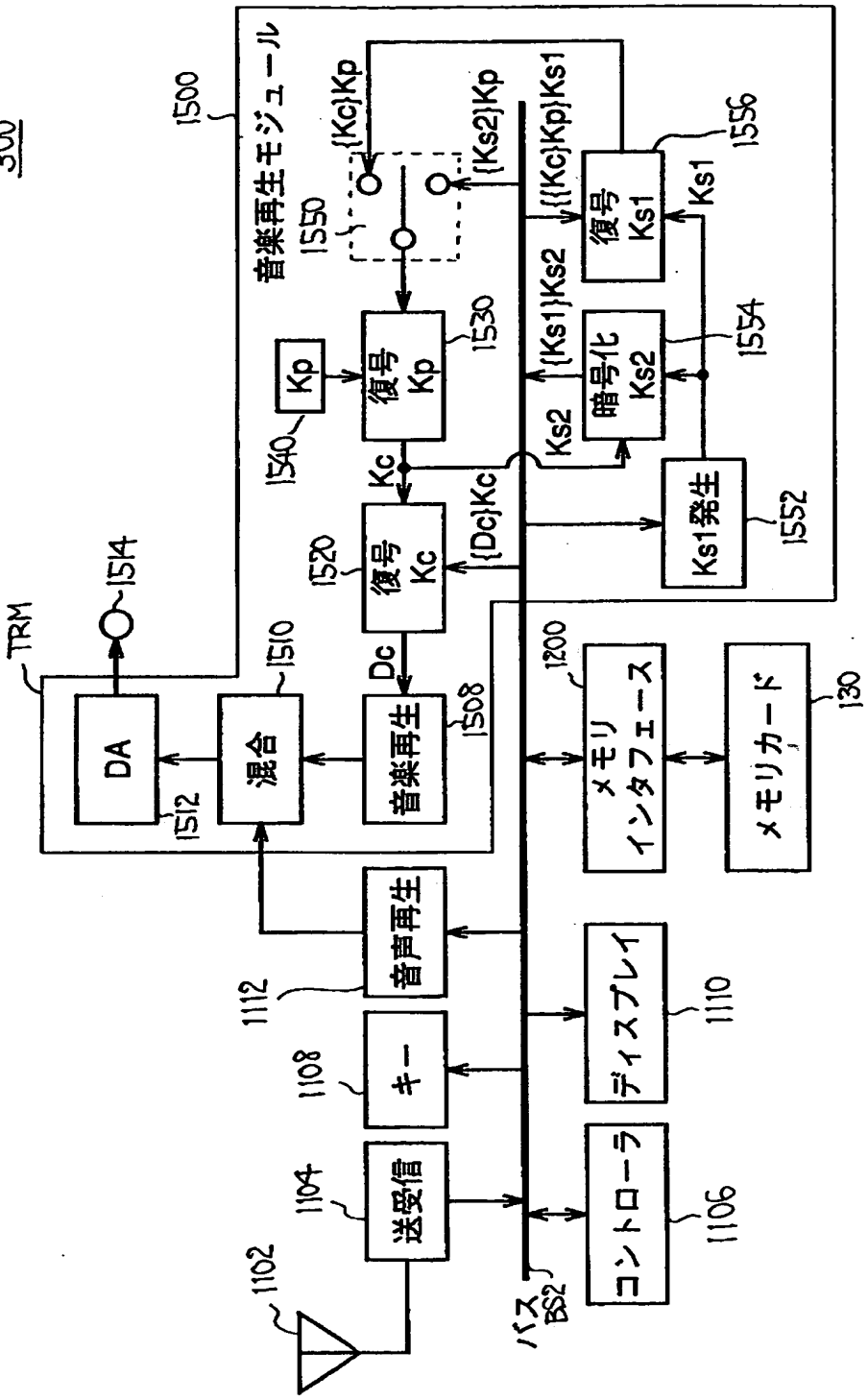
【図６】


1401
1406
1404
1402
KPm
暗号
Ks
Ks
復号
Km
Km
BS3
1202
コントローラ
1420
メモリ
暗号化コンテンツキー
{Kc}Kp
1412
暗号化音楽データ
{Dc}Kc
メモリカード
120

【図７】


携帯電話機200
メモリカード120
開始
利用者による再生指示
S200
公開暗号化キーKPmを出力
S202
公開暗号化キーKPmを獲得
S204
セッションキーKsを生成
S206
セッションキーKsを、公開暗号化キーKPmにて暗号化
(暗号化セッションキー{Ks}Kmの生成)
S208
暗号化セッションキー{Ks}Kmを復号キーKmにて復号
(Ksの獲得)
S210
暗号化コンテンツキー{Kc}Kpをメモリから読み出し
S212
暗号化コンテンツキー{Kc}Kpをセッションキー{Ks}Kmにて暗号化
(暗号化されたKpの生成)
S214
暗号化音楽データ{Dc}Kcをメモリから読み出し
S222
暗号化されたKpを固有の秘密復号キーKpiにて復号
(Kpの獲得)
S216
暗号化コンテンツキー{Kc}Kpを固有の秘密復号キーKpiにて復号
(コンテンツ復号キーKcの再生)
S218
Kc復号の可否
S220
否
可
暗号化音楽データ{Dc}Kcをコンテンツキー{Kc}にて復号
(音楽データDcの再生)
音楽データDcから音楽を再生
S224
終了
S226

【図８】

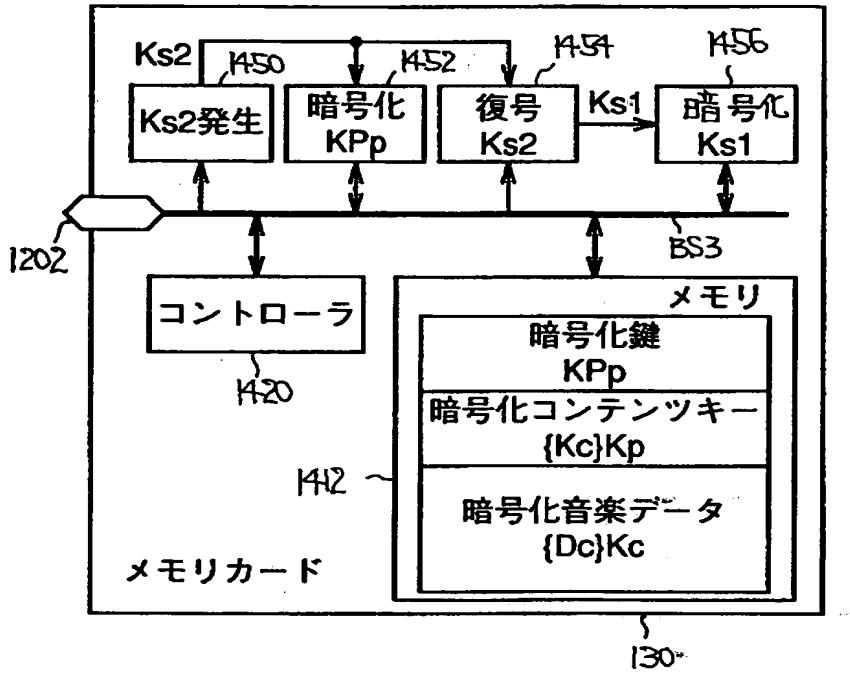

300
1500
音楽再生モジュール
{Kc}Kp
{Ks2}Kp
{{Kc}Kp}Ks1
1556
復号 Ks1
Ks1
1550
{Ks1}Ks2
1530
復号 Kp
Kp
1540
暗号化 Ks2
1554
Ks2
Kc
{Dc}Kc
Ks1発生
1552
1520
復号 Kc
1514
TRM
Dc
1510
1508
DA
混合
音楽再生
1200
メモリ インタフェース
メモリカード
130
音声再生
1112
キー
1108
ディスプレイ
1110
送受信
1104
コントローラ
1106
1102
バス BS2

【図９】

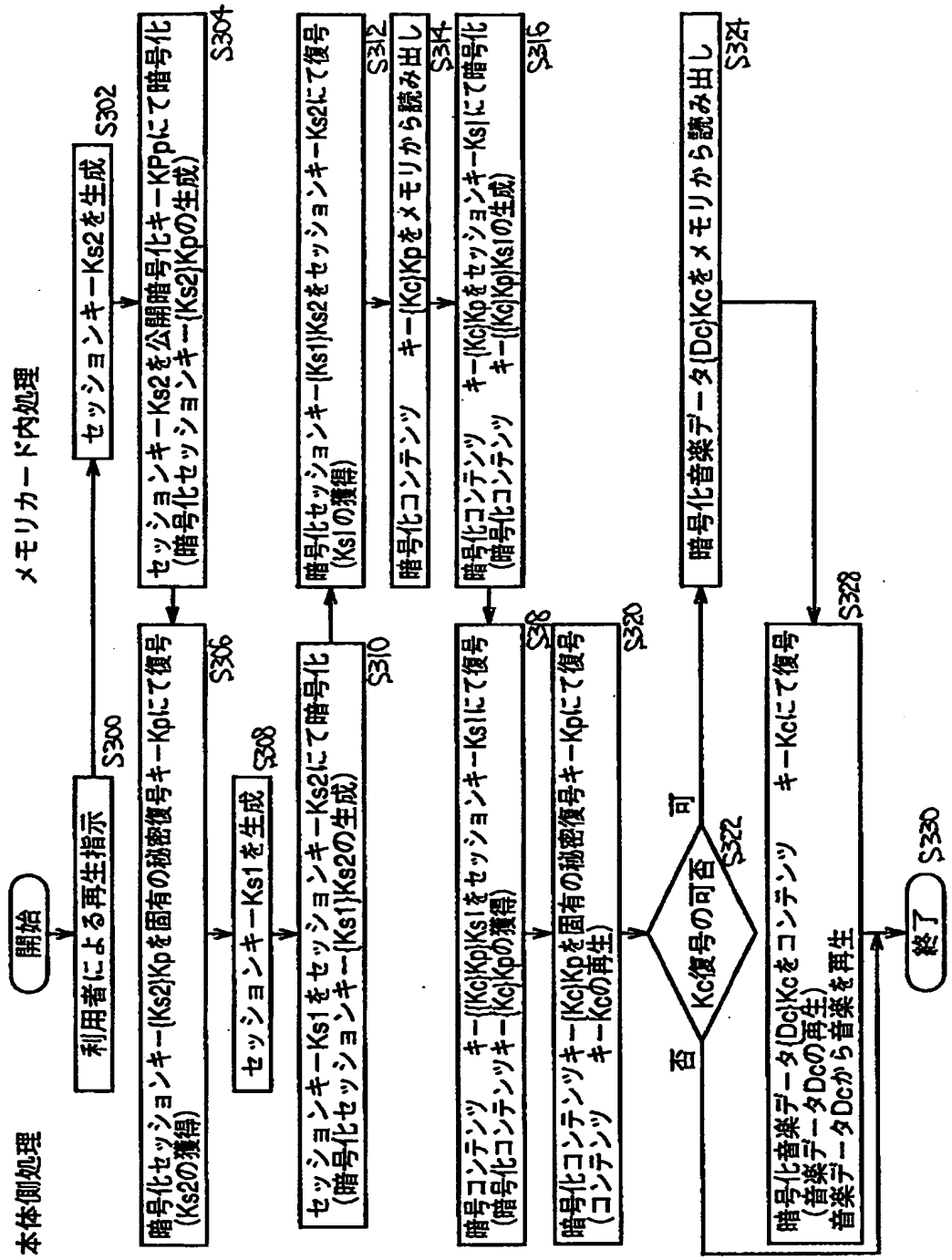
	記号	属性	特性	
メモリカード管理の鍵	Km	秘密復号鍵		メモリカード毎に異なる
	KPm	公開暗号鍵		KPmで暗号化されたデータは非対称な復号鍵Kmで復号可能
	Ks2	共通鍵	セッション固有	メモリと音楽再生モジュール間のアクセス毎に発生
音楽再生モジュール管理の鍵	Kp	秘密復号鍵	データ再生装置（携帯電話機）固有	データ再生装置毎に異なる
	Ks1	共通鍵	セッション固有	メモリと音楽再生モジュール間のアクセス毎に発生
配信データ	KPp	公開暗号鍵		KPpで暗号化されたデータは非対称な復号鍵Kpで復号可能
	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

【図１０】

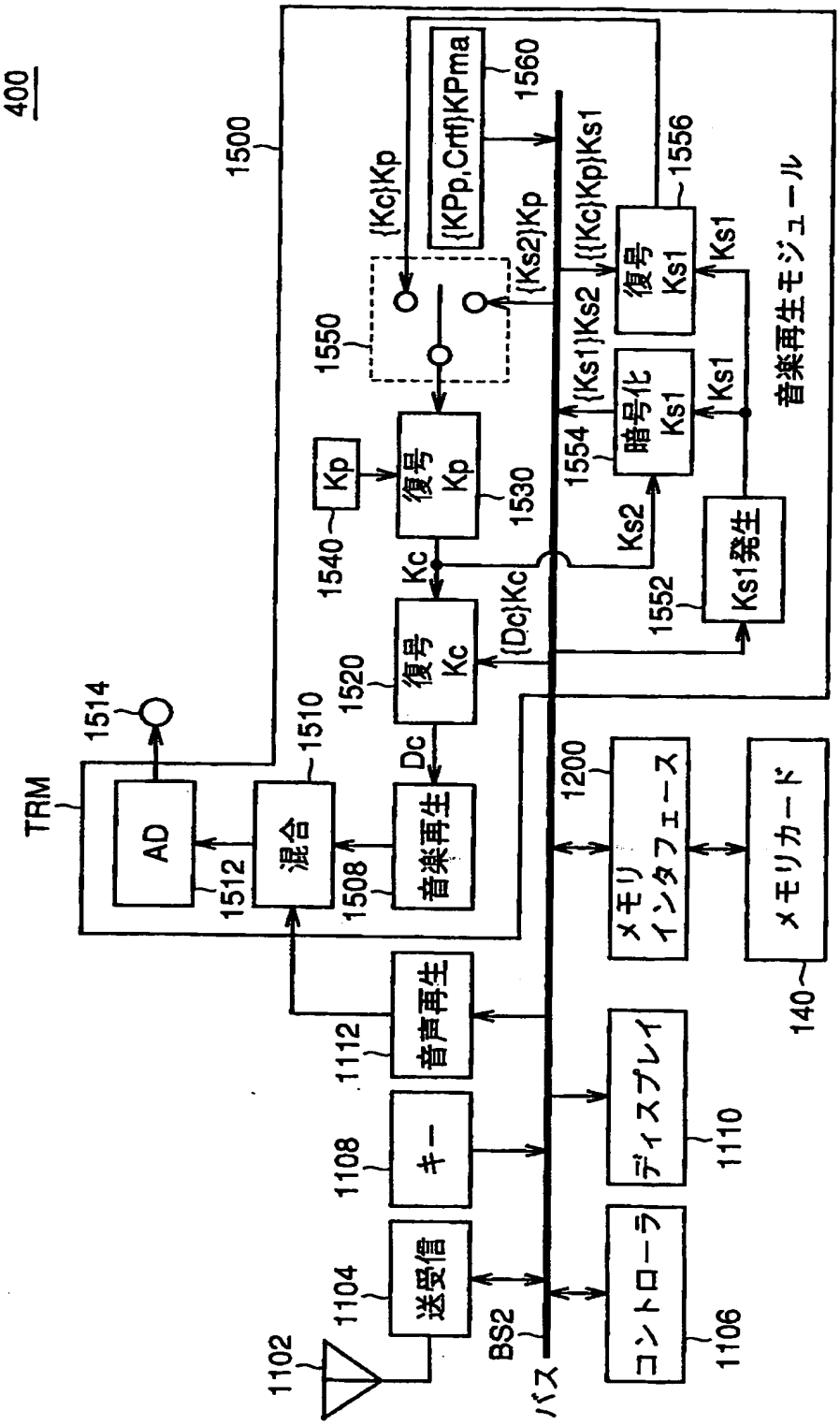
メモリカード内の構造



【図１１】


本体側処理
メモリカード内処理
開始
利用者による再生指示
S300
セッションキーKs2を生成
S302
セッションキーKs2を公開暗号化キーKPpにて暗号化
(暗号化セッションキー{Ks2}Kpの生成)
S304
暗号化セッションキー{Ks2}Kpを固有の秘密復号キーKpにて復号
(Ks2の獲得)
S306
セッションキーKs1を生成
S308
セッションキーKs1をセッションキーKs2にて暗号化
(暗号化セッションキー{Ks1}Ks2の生成)
S310
暗号化セッションキー{Ks1}Ks2をセッションキーKs2にて復号
(Ks1の獲得)
S312
暗号化コンテンツ　キー{Kc}Kpをメモリから読み出し
S314
暗号化コンテンツ　キー{Kc}Kpをセッションキーks1にて暗号化
(暗号化コンテンツ　キー{{Kc}Kp}Ks1の生成)
S316
暗号コンテンツ　キー{{Kc}Kp}Ks1をセッションキーKs1にて復号
(暗号化コンテンツキー{Kc}Kpの獲得)
S318
暗号化コンテンツキー{Kc}Kpを固有の秘密復号キーKpにて復号
(コンテンツ　キーKcの再生)
S320
Kc復号の可否
S322
否
可
暗号化音楽データ{Dc}Kcをメモリから読み出し
S324
暗号化音楽データ{Dc}Kcをコンテンツ　キーKcにて復号
(音楽データDcの再生)
音楽データDcから音楽を再生
S328
終了
S330

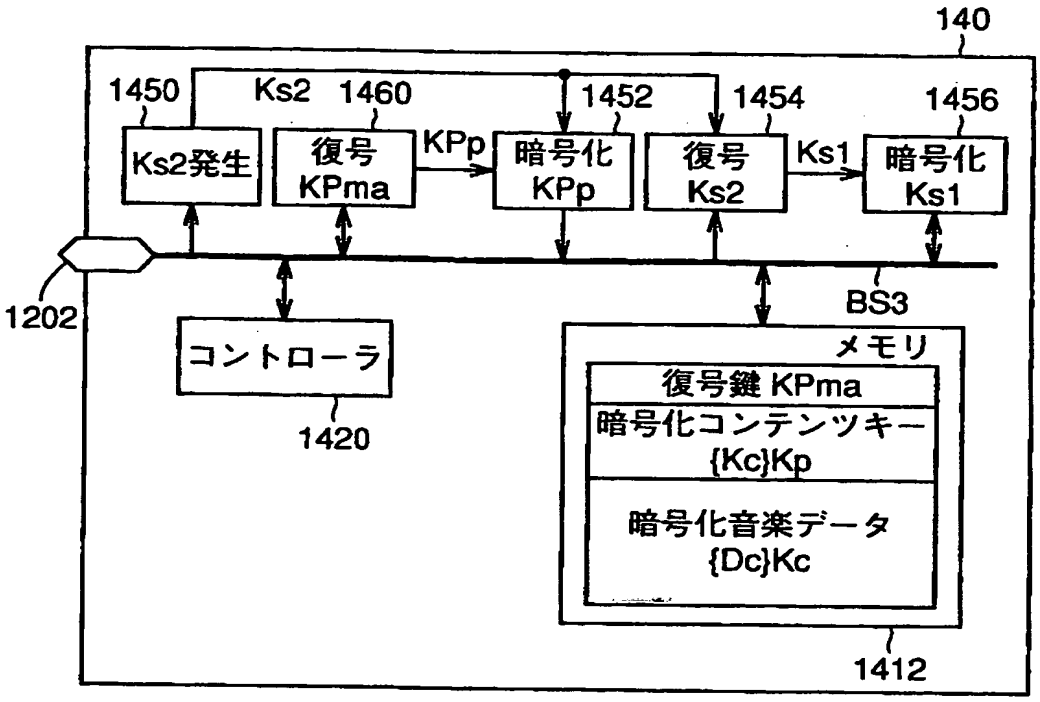
【図１２】


400
1500
音楽再生モジュール
TRM
1514
AD
1512
1510
混合
1508
音楽再生
Dc
1520
復号 Kc
Kc
1540
Kp
復号 Kp
1530
1550
{Kc}Kp
{KPp,Crtf}KPma
1560
{Ks2}Kp
{{Kc}Kp}Ks1
1556
復号 Ks1
Ks1
{Ks1}Ks2
1554
暗号化 Ks1
Ks1
Ks2
Ks1発生
1552
{Dc}Kc
1200
メモリ インタフェース
メモリカード
140
音声再生
1112
キー
1108
ディスプレイ
1110
送受信
1104
コントローラ
1106
1102
BS2
バス

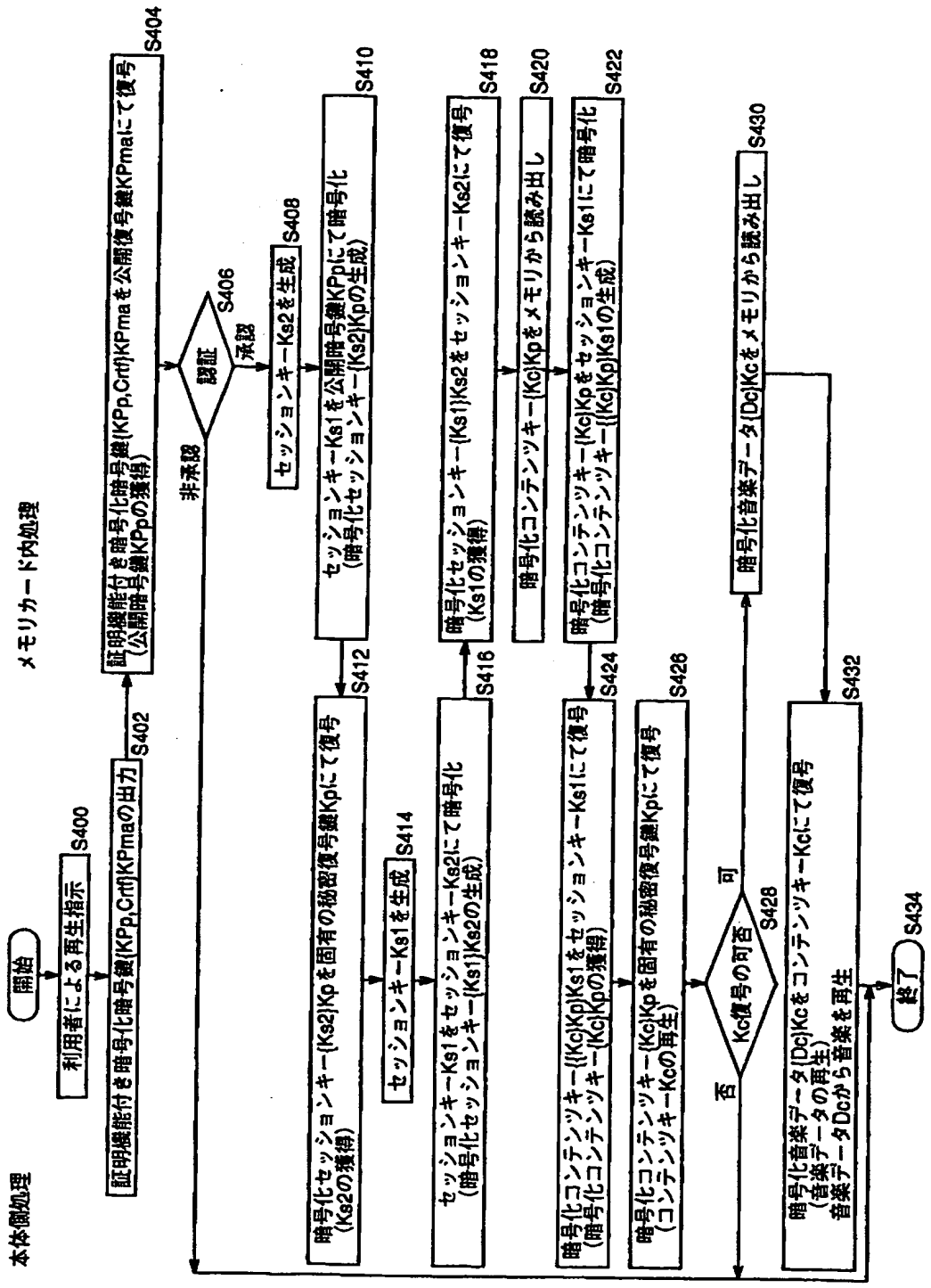
【図１３】

	記号	属性	特性	
メモリカード管理の鍵	KPma	公開復号鍵	システム共通	{KPp,Cnt}KPmaの復号によってKPpの認証を行う機能を有する認証鍵
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール艦のアクセス毎に発生
音楽生成モジュール管理の鍵	KPp	公開暗号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

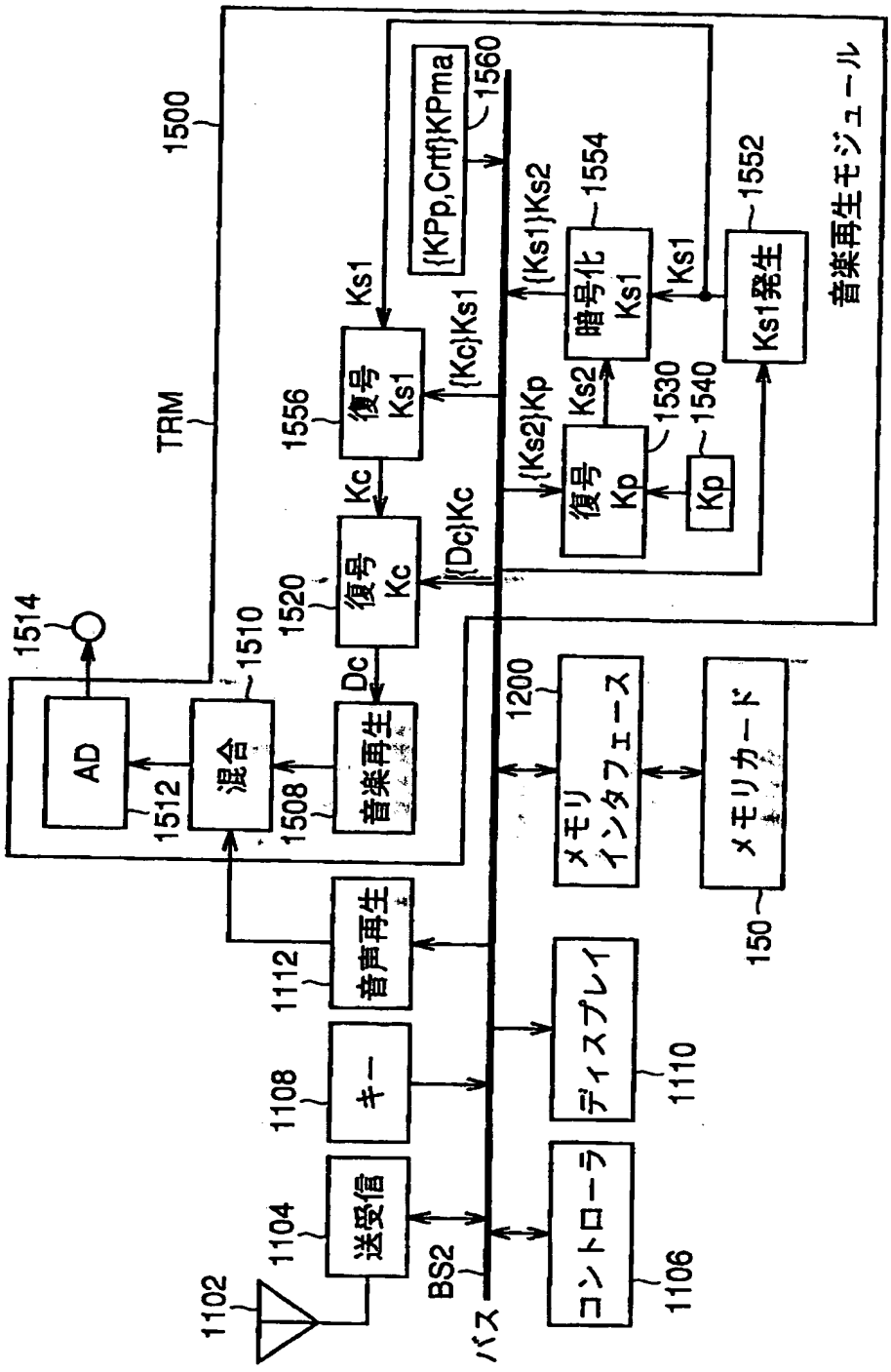
【図１４】


140
1450
Ks2
1460
1452
1454
1456
Ks2発生
復号
KPma
KPp
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
BS3
コントローラ
1420
メモリ
復号鍵 KPma
暗号化コンテンツキー
{Kc}Kp
暗号化音楽データ
{Dc}Kc
1412

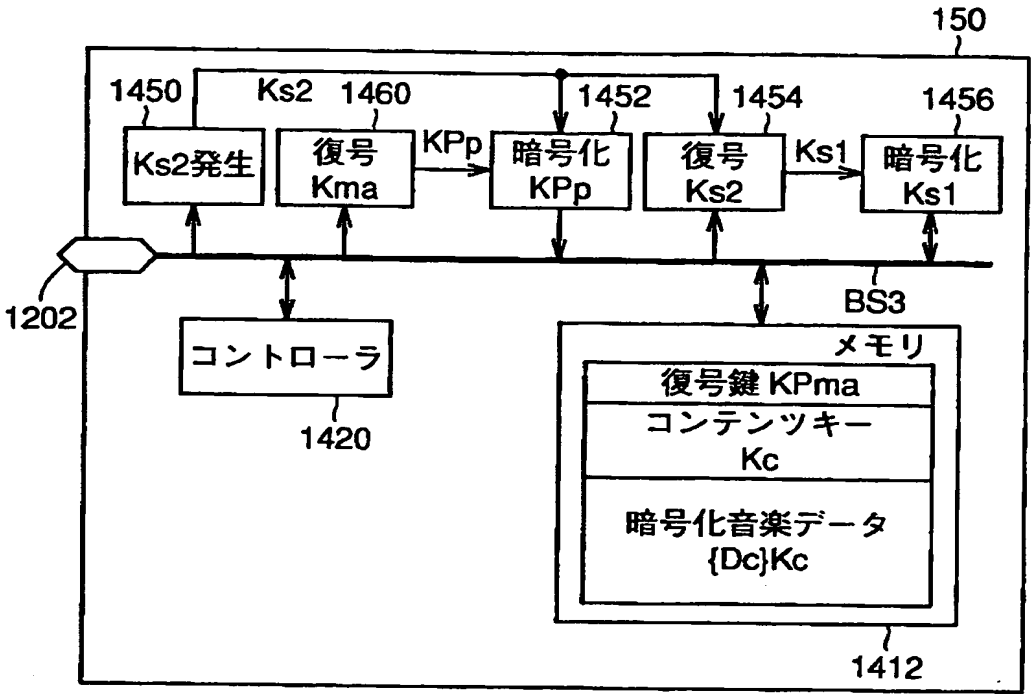
【図１５】


本体側処理
メモリカード内処理
開始
利用者による再生指示
S400
証明機能付き暗号化暗号鍵(KPp,Cnt)KPmaの出力
S402
証明機能付き暗号化暗号鍵(KPp,Cnt)KPmaを公開復号鍵KPmaにて復号
(公開暗号鍵KPpの獲得)
S404
認証
S406
非承認
承認
セッションキーKs2を生成
S408
セッションキーKs1を公開暗号鍵KPpにて暗号化
(暗号化セッションキー(Ks2)Kpの生成)
S410
暗号化セッションキー(Ks2)Kpを固有の秘密復号鍵Kpにて復号
(Ks2の獲得)
S412
セッションキーKs1を生成
S414
セッションキーKs1をセッションキーKs2にて暗号化
(暗号化セッションキー(Ks1)Ks2の生成)
S416
暗号化セッションキー(Ks1)Ks2をセッションキーKs2にて復号
(Ks1の獲得)
S418
暗号化コンテンツキー(Kc)Kpをメモリから読み出し
S420
暗号化コンテンツキー(Kc)Kpをセッションキーks1にて暗号化
(暗号化コンテンツキー{(Kc)Kp}Ks1の生成)
S422
暗号化コンテンツキー{(Kc)Kp}Ks1をセッションキーKs1にて復号
(暗号化コンテンツキー(Kc)Kpの獲得)
S424
暗号化コンテンツキー(Kc)Kpを固有の秘密復号鍵Kpにて復号
(コンテンツキーKcの再生)
S426
Kc復号の可否
S428
否
可
暗号化音楽データ(Dc)Kcをメモリから読み出し
S430
暗号化音楽データ(Dc)Kcをコンテンツキーkcにて復号
(音楽データDcの再生)
音楽データDcから音楽を再生
S432
終了
S434

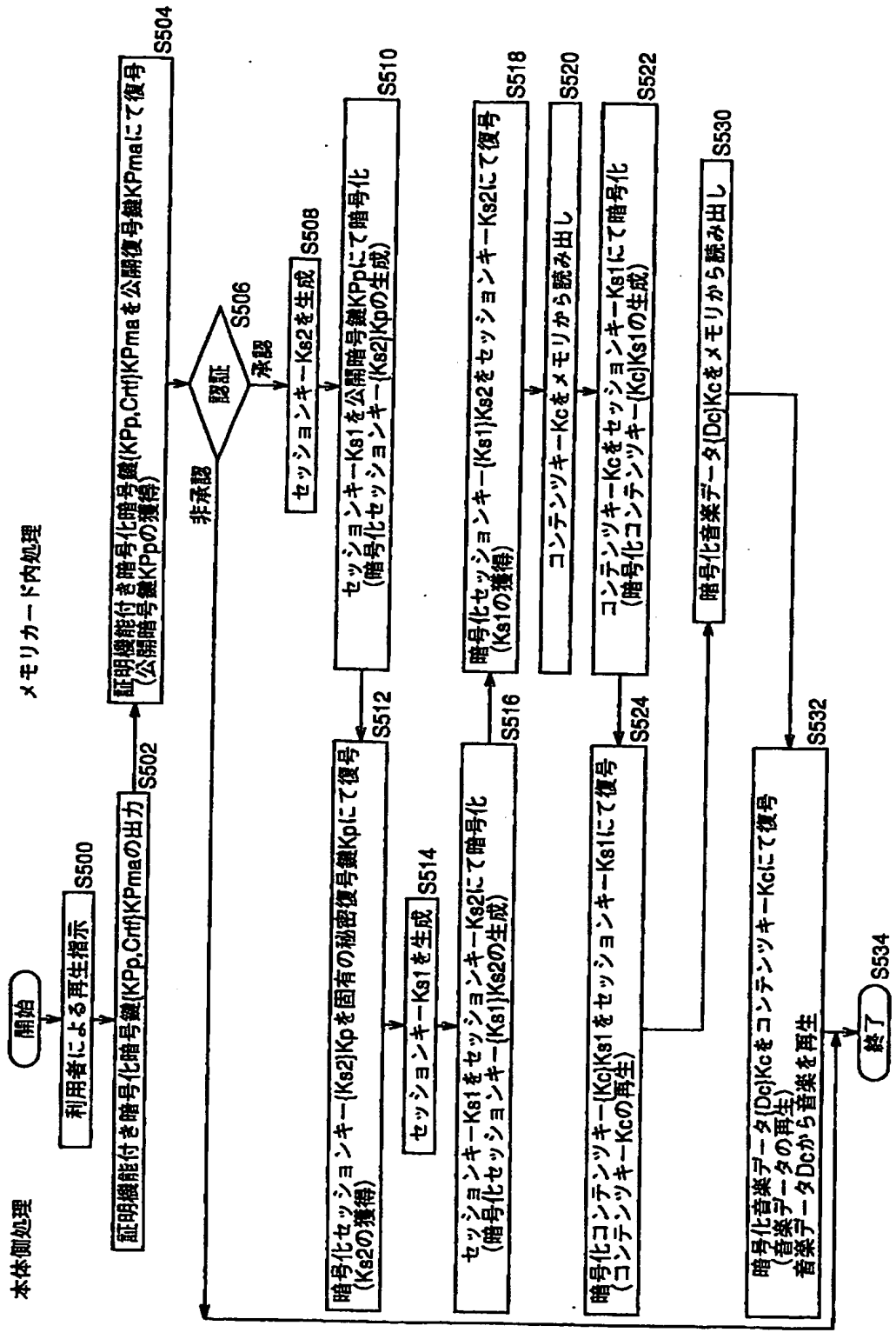
【図１６】


500
1500
TRM
音楽再生モジュール
1514
AD
1512
1510
混合
1508
音楽再生
Dc
1520
復号
Kc
Kc
1556
復号
Ks1
Ks1
{Kc}Ks1
{Dc}Kc
{Ks2}Kp
Ks2
1530
復号
Kp
1540
Kp
{Ks1}Ks2
1554
暗号化
Ks1
Ks1
1552
Ks1発生
{KPp,Cnt}KPma
1560
1200
メモリ
インタフェース
メモリカード
150
音声再生
1112
キー
1108
ディスプレイ
1110
送受信
1104
コントローラ
1106
1102
BS2
バス

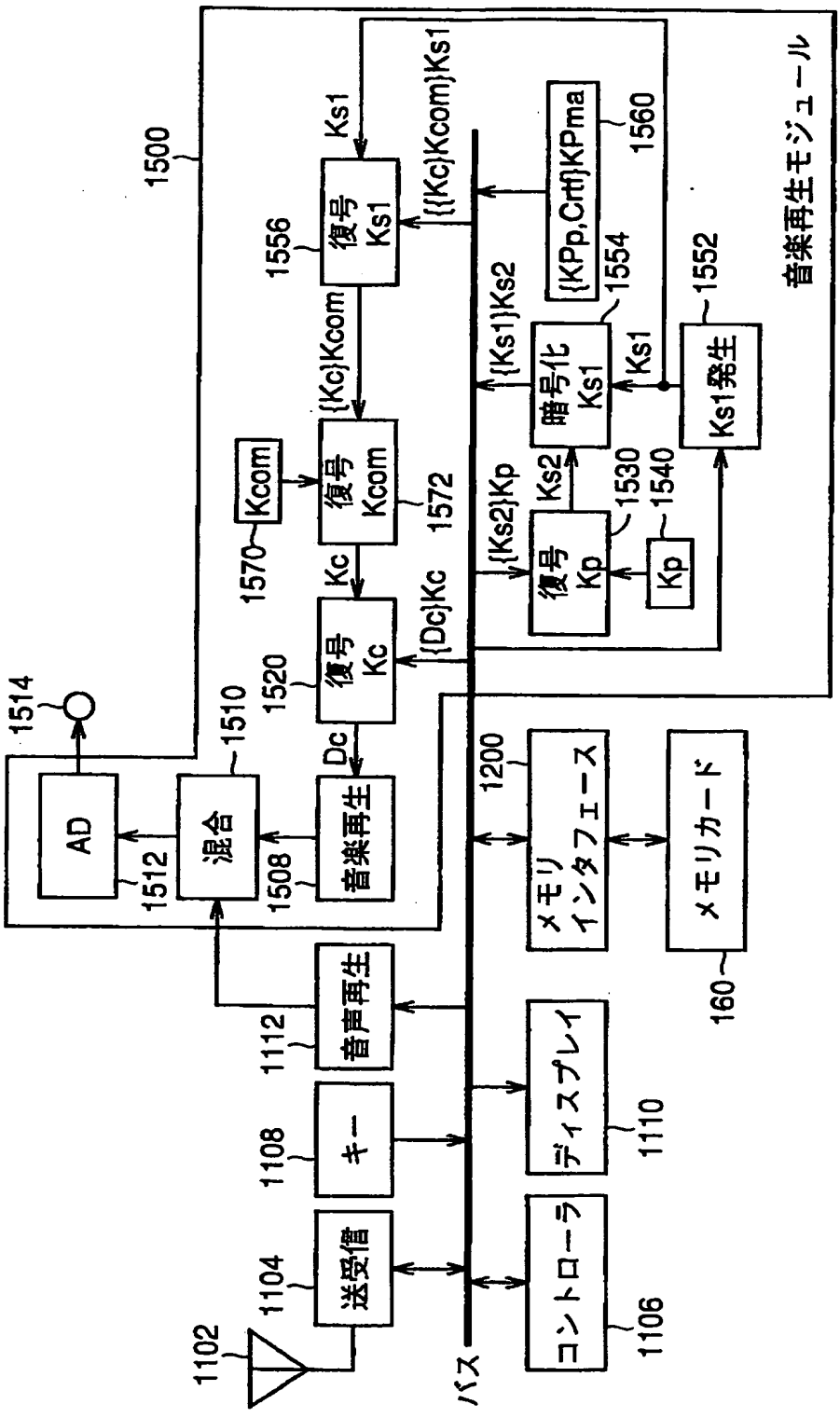
【図１７】


150
1450
Ks2
1460
1452
1454
1456
Ks2発生
復号
Kma
KPp
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
BS3
コントローラ
1420
メモリ
復号鍵 KPma
コンテンツキー
Kc
暗号化音楽データ
{Dc}Kc
1412

【図１８】


本体側処理
メモリカード内処理
開始
利用者による再生指示
S500
証明機能付き暗号化暗号鍵(KPp,Cnf)KPmaの出力
S502
証明機能付き暗号化暗号鍵(KPp,Cnf)KPmaを公開復号鍵KPmaにて復号
(公開暗号鍵KPpの獲得)
S504
認証
S506
非承認
承認
セッションキーKs2を生成
S508
セッションキーKs1を公開暗号鍵KPpにて暗号化
(暗号化セッションキー(Ks2)Kpの生成)
S510
暗号化セッションキー(Ks2)Kpを固有の秘密復号鍵Kpにて復号
(Ks2の獲得)
S512
セッションキーKs1を生成
S514
セッションキーKs1をセッションキーKs2にて暗号化
(暗号化セッションキー(Ks1)Ks2の生成)
S516
暗号化セッションキー(Ks1)Ks2をセッションキーKs2にて復号
(Ks1の獲得)
S518
コンテンツキーKcをメモリから読み出し
S520
コンテンツキーKcをセッションキーKs1にて暗号化
(暗号化コンテンツキー(Kc)Ks1の生成)
S522
暗号化コンテンツキー(Kc)Ks1をセッションキーKs1にて復号
(コンテンツキーKcの獲得)
S524
暗号化音楽データ(Dc)Kcをメモリから読み出し
S530
暗号化音楽データ(Dc)Kcをコンテンツキー Kcにて復号
(音楽データの再生)
音楽データDcから音楽を再生
S532
終了
S534

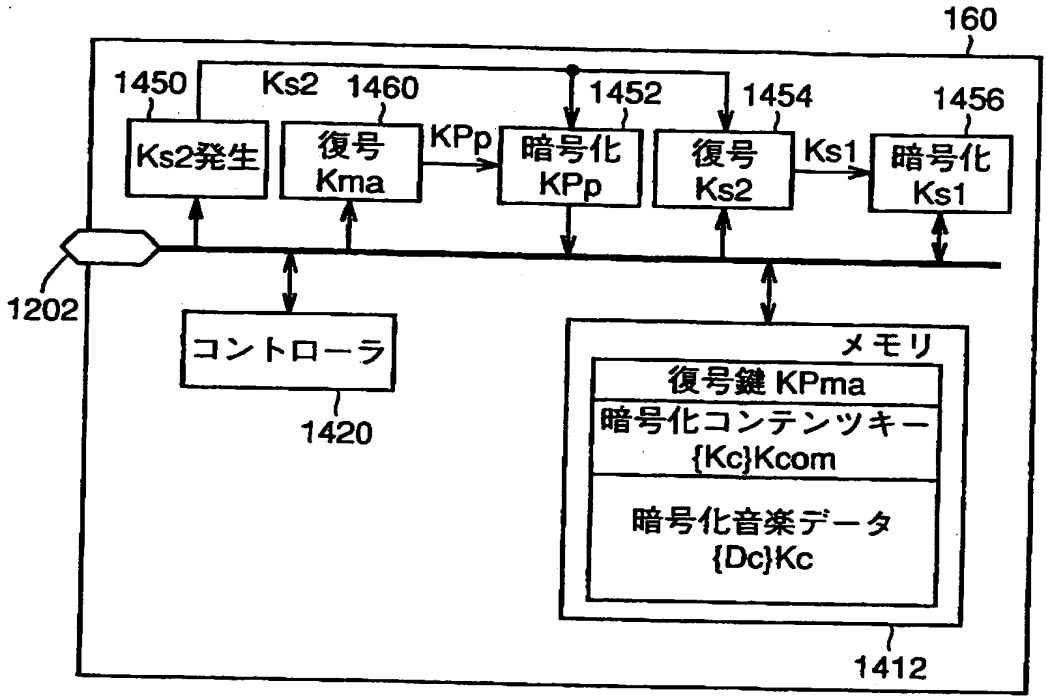
【図１９】


600
1500
音楽再生モジュール
1514
AD
1512
1510
混合
1508
音楽再生
Dc
1520
復号
Kc
{Dc}Kc
Kc
1570
Kcom
復号
Kcom
1572
{Kc}Kcom
1556
復号
Ks1
Ks1
{{{Kc}Kcom}Ks1
{Ks2}Kp
復号
Kp
1530
Ks2
Kp
1540
{Ks1}Ks2
暗号化
Ks1
1554
Ks1
Ks1発生
1552
{{KPp,Crtf}KPma
1560
1200
メモリ
インタフェース
メモリカード
160
1112
音声再生
1108
キー
1110
ディスプレイ
1104
送受信
1106
コントローラ
1102
バス

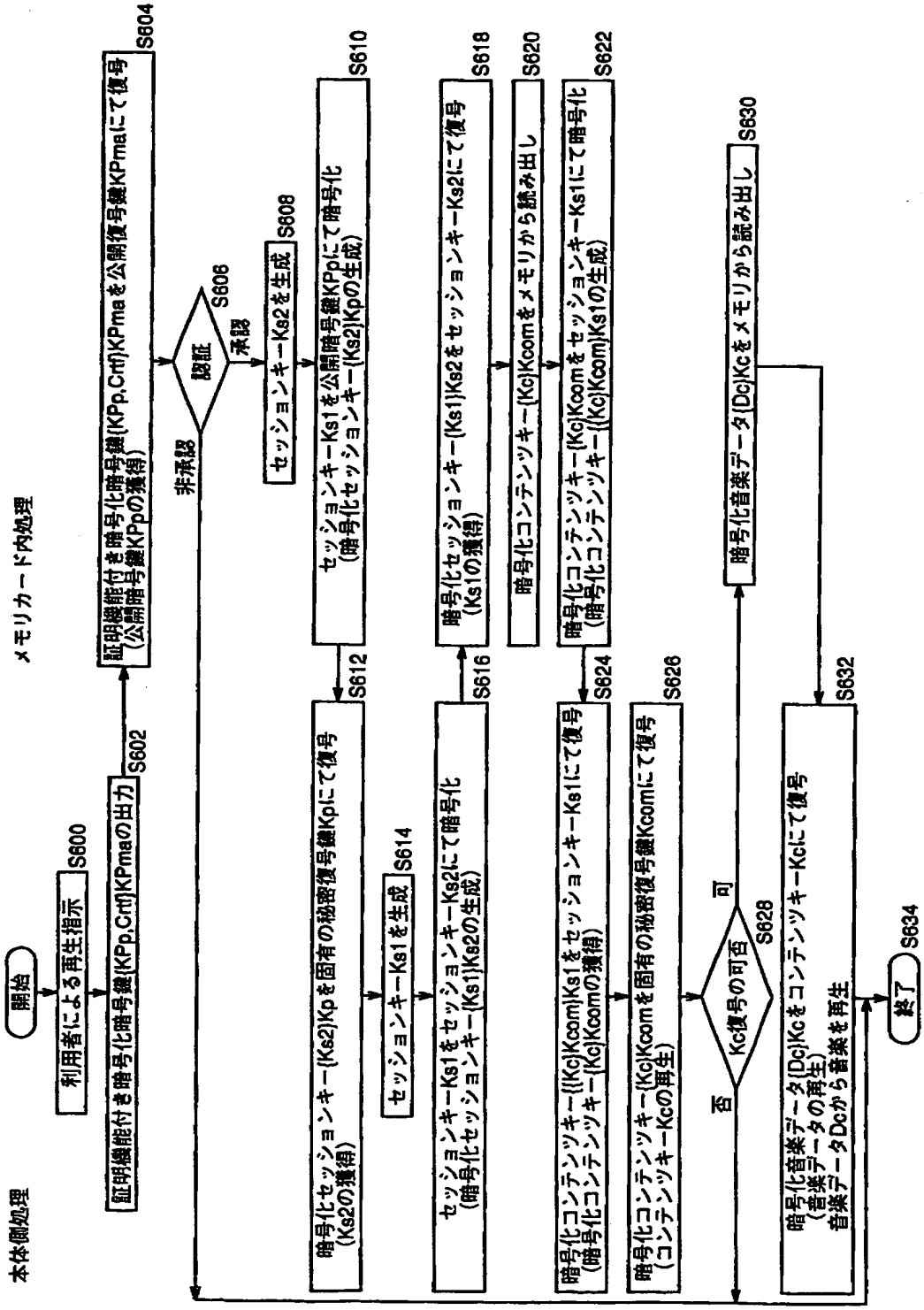
【図２０】

	記号	属性	特性	
メモリカード管理の鍵	KPma	公開復号鍵	システム共通	{KPp}KPmaの復号によってKPpの認証を行う機能を有する認証鍵
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール艦のアクセス毎に発生
音楽生成モジュール管理の鍵	KPp	公開暗号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス(種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Kcom	秘密復号鍵	システム共通	暗号化されたコンテンツキーを復号する
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

【図２１】


160
1450
Ks2
1460
1452
1454
1456
Ks2発生
復号
Kma
KPp
暗号化
KPp
復号
Ks2
Ks1
暗号化
Ks1
1202
コントローラ
1420
メモリ
復号鍵 KPma
暗号化コンテンツキー
{Kc}Kcom
暗号化音楽データ
{Dc}Kc
1412

【図２２】


本体側処理
メモリカード内処理
開始
利用者による再生指示
S600
証明機能付き暗号化(KPp,Cmf)KPmaの出力
S602
証明機能付き暗号化暗号鍵(KPp,Cmf)KPmaを公開復号鍵KPmaにて復号
(公開暗号鍵KPpの獲得)
S604
認証
S606
非承認
承認
セッションキーKs2を生成
S608
セッションキーKs1を公開暗号鍵KPpにて暗号化
(暗号化セッションキー(Ks2)Kpの生成)
S610
暗号化セッションキー(Ks2)Kpを固有の秘密復号鍵Kpにて復号
(Ks2の獲得)
S612
セッションキーKs1を生成
S614
セッションキーKs1をセッションキーKs2にて暗号化
(暗号化セッションキー(Ks1)Ks2の生成)
S616
暗号化セッションキー(Ks1)Ks2をセッションキーKs2にて復号
(Ks1の獲得)
S618
暗号化コンテンツキー(Kc)Kcomをメモリから読み出し
S620
暗号化コンテンツキー(Kc)Kcomをセッションキーks1にて暗号化
(暗号化コンテンツキー((Kc)Kcom)Ks1の生成)
S622
暗号化コンテンツキー((Kc)Kcom)Ks1をセッションキーKs1にて復号
(暗号化コンテンツキー(Kc)Kcomの獲得)
S624
暗号化コンテンツキー(Kc)Kcomを固有の秘密復号鍵Kcomにて復号
(コンテンツキーKcの再生)
S626
Kc復号の可否
S628
否
可
暗号化音楽データ(Dc)Kcをメモリから読み出し
S630
暗号化音楽データ(Dc)Kcをコンテンツキーkcにて復号
(音楽データの再生)
音楽データDcから音楽を再生
S632
終了
S634

【書類名】　　要約書

【要約】

【課題】　許可なく著作権物データにアクセスされることを防止することが可能なデータ再生装置を提供する。

【解決手段】　携帯電話機１００は、配信された暗号化コンテンツデータおよび暗号化コンテンツキーをメモリ１１０に格納する。メモリ１１０から読み出された暗号化コンテンツキーデータは、Ｋｐ保持部１５４０の保持するキーデータＫｐにより復号処理部１５３０により復号されて、音楽再生モジュール１５００に取り込まれる。復号処理部１５２０は、メモリ１１０から読み出した暗号化コンテンツデータを、復号処理部１５３０により抽出されたコンテンツキーＫｃにより復号して、コンテンツデータＤｃを再生する。

【選択図】　　図２

認定・付加情報

特許出願の番号	平成１１年　特許願　第３４３７０７号
受付番号	５９９０１１７８４６７
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１２年　２月１０日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000005223
- 【住所又は居所】 神奈川県川崎市中原区上小田中４丁目１番１号
- 【氏名又は名称】 富士通株式会社

【特許出願人】
- 【識別番号】 000004167
- 【住所又は居所】 東京都港区赤坂４丁目１４番１４号
- 【氏名又は名称】 日本コロムビア株式会社

【特許出願人】
- 【識別番号】 000001889
- 【住所又は居所】 大阪府守口市京阪本通２丁目５番５号
- 【氏名又は名称】 三洋電機株式会社

【代理人】 申請人
- 【識別番号】 100064746
- 【住所又は居所】 大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 深見　久郎

【選任した代理人】
- 【識別番号】 100085132
- 【住所又は居所】 大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 森田　俊雄

【選任した代理人】
- 【識別番号】 100091409
- 【住所又は居所】 大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
- 【氏名又は名称】 伊藤　英彦

【選任した代理人】

次頁有

認定・付加情報（続き）

【識別番号】　100096781
【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　堀井　豊

次頁無

出 願 人 履 歴 情 報

識別番号　〔０００００１８８９〕

１．変更年月日　１９９３年１０月２０日
［変更理由］　住所変更
住　所　大阪府守口市京阪本通２丁目５番５号
氏　名　三洋電機株式会社